GRAPHICAL DATA

Security of Apps and Business (Cloud Hosted)

Service Overview

The application is a subscription based software product for managing workflow and business processes (Resolve). It is a cloud based solution and so will be accessible through the internet.

The Resolve system runs on Amazon Web Services (AWS), including the EC2 (Elastic Compute Cloud) and S3 Simple Storage Service. The Resolve software therefore benefits from the security best practices, certifications and audits which Amazon adheres to in it's AWS service. AWS uses comprehensive security capabilities to satisfy the most demanding information security requirements.

Security Organisation and Policy

Qu. Are any employees within your organisation solely dedicated to Security?

> This responsibility is shared between a number of core managers. Security of our cloud based service is overseen by our Technical Director.
>
> Information and data security as a function is organized centrally and overseen by a core team of senior managers whose responsibility it is to ensure our Information Security policies are maintained and enforced throughout the organization. Some of our information system functions are presently outsourced to Amazon Web Services, including hosting of Graphical Data Cloud services for customer use.

QU. Do you do personnel screening for employees and contractors.

Graphical Data do operate a standard screening process when hiring any employees or contractors. The standards we require from each prospective employee are:

- application, CV details, background (experience, qualifications)
- interviews to verify suitability.
- professional references from at least 2 employers
- identity must be verified by appropriate means (license/passport)
- criminal record background check on all potential employees and
- contractors or Basic Criminal Disclosure.

QU. Do you have a security awareness program with employees and contractors?

Graphical Data operate monthly reviews attended by all employees to discuss any recent incidents, concerns and/or policy queries. Policy documentation is available to all employees via the GD intranet.

Graphical Data has not suffered information security related incidents over the past two years?

QU. Do you have defined and documented escalation procedure for fault management and major incident / security incident handling?

Internally

All incidents or problems are received, dealt with and recorded by our Service Desk and system. The incident or problem is identified and classified into the appropriate severity level (Low, Medium, High and Critical) using the information gathered from the notification. When the nature of the issue and its severity level have been determined, the resolution process begins - it is sent to the appropriate owner. If possible, the issue will be corrected quickly. However, if the nature of the problem means it may take some time to properly investigate, the first objective is to find a workaround solution. If an issue is identified as being a major incident, extra resource will be brought in to deal appropriately, including Service Manager and/or Technical Director.

All issues are recorded and kept on our internal system, enabling auditing and reporting.

AWS Procedures

For incidents, vulnerabilities and threats that impact the AWS Data Center, the Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business impacting events.

Amazon's incident response program, plans and procedures have been developed in alignment with ISO27001 standard.

QU. Do you have a documented security policy and/or standards to deliver security requirements appropriate for the service and its operation.

Yes, GD have internal guidelines which include statements on the following:

- Information Security, including Data Storage, Processing and Transmission guidelines.
- Resiliency Plans, including Data, Applications and Operations (hardware and software).

- Security Information - physical and infrastructure security, employee training etc.
- Software Development - procedures that should be followed to ensure secure and stable software, testing and validation methods to be used, identify who is responsible for managing and maintaining these
- Auditing and Performance Measuring - protecting, securing and auditing access to sensitive resources, measuring response times and rate of defining and addressing issues, fault management.

AWS's Compliance and Security teams have established and information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls.

Amazon maintains the security policy, provides security training to employees and performs application security reviews. These reviews assess the confidentiality, integrity and availability of the data, as well as conformance to the information security policy.

GD's own Security policy adheres as much as possible to the principles set out in ISO27001, ITIL Best Practices and the Open Web Application Security Project. **GD are ISO27001 accredited**.

Amazon framework based on:

- COBIT
- ISO27000
- AICPA
- PCI DSS v2.0
- NISTQU.

Qu. Do your employees (permanent, temporary and contract) sign a document indicating they have read and understood your organisations security and privacy policies?

All employees are required to complete a security policy induction, which is regularly followed up during our monthly reviews. All staff employment or contracts for service specifically refer to compliance with the GD Staff Handbook, which includes our Security and Privacy policies

Background checking and vetting measures undertake on employees and subcontractors of GD include:

Verification checks are performed on all applicants for permanent employment as follows:

- Employee applications, CV details, experience, and qualifications must be matched against a job description to verify the potential suitability of the applicant;

- Interviews must be conducted on an individual basis to verify suitability. Formal offers of employment may only be made to an individual subject to the following checks being made:

- Character and professional references must be confirmed by obtaining two employer references;

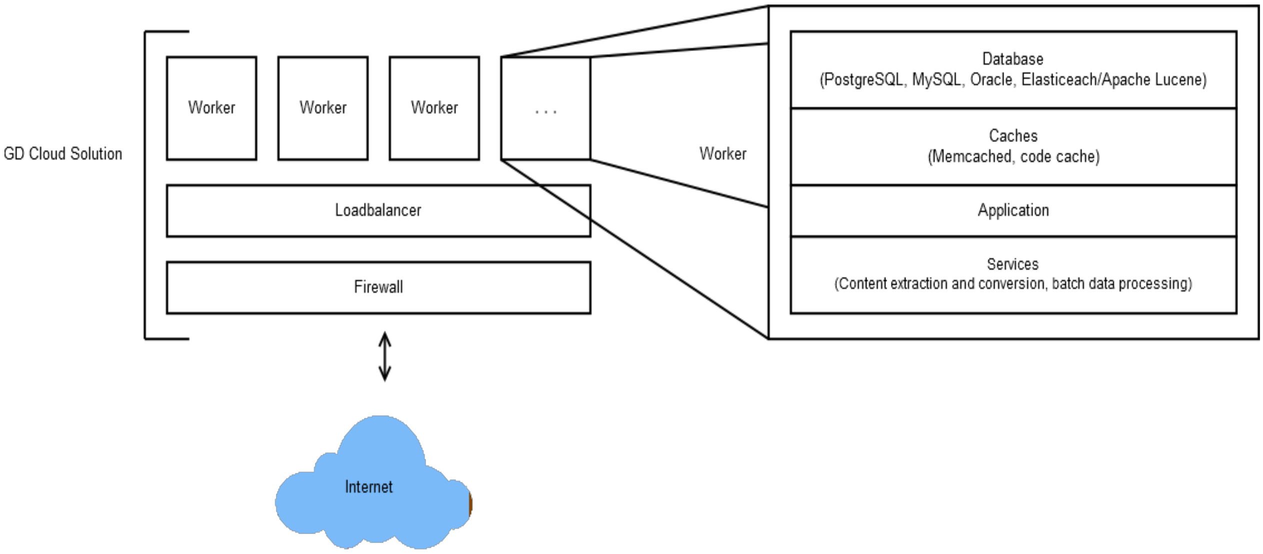
- Academic and professional qualifications must be confirmed by requesting original printed copies of the most relevant qualifications;

- An applicant's identity must be verified via a passport or a driving licence.

Service Architecture

The service consists of a number of application workers hosted on Amazon Web Services which provide an interface to the Resolve application over HTTP(S). Each worker is a standalone virtual machine which, at its minimal, contains an execution server, Resolve application and a data cache. It can also contain an internal database server is a strict data isolation is needed this is the case for Smart Metering Resolve). All traffic directed at the application first goes through a firewall and only genuine requests are passed to a load balancer which then decides what worker should process the request.

Logical architecture of the service can be summarised by the below diagram



Customer Data Security

Qu. Who; in terms company or subcontractors, will be involved in processing the data provided by the customer

The following Graphical Data employees will be able to access information supplied and owned by the client:

(GD Technical Director)

(GD Managing Directions)

(Operations, Data Management)

For more information, please contact info@graphicaldata.co.uk

Qu. Where external or third-party companies are used, please provide connection & network topology diagrams

AWS is our hosting platform provider - all connections are made using SSH and SSL management in order to work on the Resolve infrastructure hosted on AWS.

Qu. Please provide detail of where (geographic locations and physical/logical technical equipment) and how Client data will be processed.

All customer data is processed and stored through Amazon Web Services. Amazon's data centers are state of the art, utilizing innovative architectural and engineering approaches.

Data centers are built in clusters in various global regions. Customer data is stored in designated physical regions. No data is replicated outside of the chosen region. The Resolve application uses the EU region and so no customer data will be transferred to data centers outside of the EU. Within the EU, Amazon have centers in Ireland and Frankfurt.

Amazon's infrastructure has a high level of availability. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact.

All data centers are online and serving customers; no data center is "cold". In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network.

Qu. Please provide detail of where (geographic locations and physical/logical technical equipment) and how Client data will be stored (e.g. multiplex, server, platform, disk or array configuration).

All customer data is processed and stored through Amazon Web Services. Amazon's data centers are state of the art, utilizing innovative architectural and engineering approaches.

Data centers are built in clusters in various global regions. Customer data is stored in designated physical regions. No data is replicated outside of the chosen region. The Resolve application uses the EU region and so no customer data will be transferred to data centers outside of the EU. Within the EU, Amazon have centers in Ireland and Frankfurt.

Amazon's infrastructure has a high level of availability. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact.

All data centers are online and serving customers; no data center is "cold". In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network.

Qu. Please give full details of data backup procedures, including type (full, differential etc), media, schedules, locations, off-site, recovery tests etc.

All data, this includes uploaded files and database, is backed up twice during a 24 hour period. Two separate copies of each dataset exist. Primary one held in Amazon S3 and secondary on an encrypted hard drive which never leaves GD office.

Primary storage service Amazon S3 is designed to provide 99.99999% durability and 99.99% availability of objects over a given year. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. To help provide durability, Amazon S3 PUT and COPY operations synchronously store customer data across multiple facilities before returning SUCCESS. Once stored, Amazon S3 helps maintain the durability of the objects by quickly detecting and repairing any lost redundancy.

Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

Amazon S3 provides further protection via Versioning. Versioning is used to preserve, retrieve, and restore every version of every object stored in an Amazon S3 bucket.

Secondary storage service is a dedicated set of SATA hard drives connected in RAID1 configuration and S.M.A.R.T. enabled.

Qu. Where client customer data is stored, is it encrypted at all times? Please provide details in either case.

Customer data (that is file uploads) stored in the Amazon S3 storage service uses Server Side Encryption (SSE) to manage the encryption process. Data is encrypted with a generated key. Data is encrypted automatically upon retrieval and can also be encrypted on upload.

Amazon S3 SSE uses one of the strongest block ciphers available - 256-bit Advanced Encryption Standard (AES-256). With Amazon S3 SSE, every protected object is encrypted with a unique key. This object itself is then encrypted with a regularly rotated master key.

Any data held in a local database (that is local to an EC2 instance) is fully encrypted at rest, using full disk encryption, and only its memory representation is unencrypted. This data held in memory can only be accessed locally by software located on a particular instance of EC2 system. Any backups of this data are stored on separate media which provide final encryption.

Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications.

AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMPsm.

Qu. How does the data storage system defend/monitor against brute force attacks?

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used so personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

Documentation is maintained to aid and inform operations personnel in handling incidents or issues. If the resolution of an issue requires collaboration, a conferencing system is used which supports communication and logging capabilities. Trained call leaders facilitate communication and progress during the handling of operational issues that require collaboration. Post-mortems are convened after any significant operational issue, regardless of external impact, and Cause of Error documents are drafted so the root cause is captured and preventative actions are taken in the future. Implementation of the preventative measures is tracked during weekly operations meetings.

Qu. What are your documented data handling, storage & disposal processes?

Examples of our standard guidelines:

Paper - Paper documents containing restricted data must be stored in a secured location such as locked office furniture, locked offices, and other locations specifically dedicated to secure storage of records when not in use. Crosscut shred or pulp all highly sensitive information in paper form including all transitory work products (e.g., unused copies, drafts, notes) to ensure physical destruction beyond ability to recover.

Removable Media - Restricted data stored on CD, DVD, BRD, or disk, must be encrypted. The media must be stored in a secured location when not in use or properly destroyed. Removable media must be destroyed by complete physical destruction of the media beyond ability to recover.

Flash Drives - Restricted data stored on a flash drive must be password protected and the data encrypted. The flash drive must be stored in a secured area when not in use or data properly destroyed. If the flash drive is going to be repurposed or destroyed, then the electronic storage device must be wiped with a multiple pass secure overwrite prior to being repurposed.

Electronic Documents - Anyone with access to electronic documents that contain restricted data must comply with the following requirements:

1. Enable password protection using a strong complex password.

2. Enabled full disk encryption to protect from data theft.

Electronic documents are properly deleted, omitting trash-bin, from the workstation when no longer needed. Hard drives being repurposed must be wiped with a multiple pass secure overwrite prior to being repurposed.

AWS:

Disposal

When an AWS storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program

Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned storage devices are degaussed and physically destroyed in accordance with industry-standard practices

AWS storage device disposal process is regularly reviewed and assessed by independent third party auditors as a part of our continued ISO 27001 and FedRAMPsm compliance program.

Physical and Environmental Security

Qu. Is the infrastructure at all locations used for the processing and storage of client data housed in a physically secure environment?

AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely

Qu. What system(s) of physical access control to the secure environment is deployed e.g. swipe cards, PIN code, and biometric readers?

AWS

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Qu. Are all accesses logged and retained with the individual's details and a time and date stamp?

All physical access to data centers by AWS employees is logged and audited routinely.

Qu. Is this asset or infrastructure and locations protected against:

- Loss of power?

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

- Fire?

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

- Flood?

AWS data centers incorporate physical protection against environmental risks. AWS services provide customers the flexibility to store data within multiple geographical regions as well as across multiple Availability zones.

- Temperature & Humidity?

  Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Qu. Are off-site data backup storage facilities used? If yes, what physical security measures are in place and how is access controlled?

> AWS uses data replication and backup techniques as opposed to off-site data backup storage facilities. AWS application data is replicated to multiple systems within and data centre and where appropriate can be replicated across multiple centres.
>
> GD local backups are encrypted with strong ciphers and held in a detachable hard drive which after operation is held in a locked office cabinet.

Qu. Is this asset or infrastructure hosted or located at a site managed by a 3rd party?

> Asset / Infrastructure hosted on AWS only.

Internet, Network, System and Application Security

Qu. Please provide details of internet connectivity and associated architecture within your company.

> GD Fibre optic Internet connection is shared between all workstations in the office and comes through a hardware router which also serves as a first step firewall solution protecting internal infrastructure from outside threats. The appliance used for this purpose is Netgear ProSecure UTM9S

Qu. Are applications developed in line with principles such as the Security Development Lifecycle to safeguard against fundamental application vulnerabilities?

GD follows industry standard best practices when developing software both for security and maintainability. We have established our own policies for secure software which cover data accepting, processing and handling, secure user authentication and session fixation. This adheres to the principles of Security Development Lifecycle.

Qu. Are internal application level firewalls deployed and effectively managed to provide protection against internally generated attacks?

The RESOLVE application is hosted on the Amazon EC2 platform. Amazon EC2 provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny-all mode and Amazon EC2 customers must explicity open the ports needed to allow inbound traffic. The traffic can be restricted by protocol, by service port, as well as by source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block).

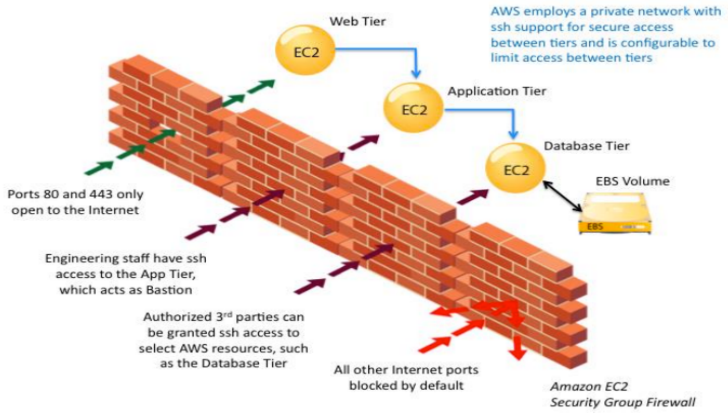

Web Tier
EC2
AWS employs a private network with ssh support for secure access between tiers and is configurable to limit access between tiers
EC2
Application Tier
Database Tier
EC2
EBS Volume
EBS
Ports 80 and 443 only open to the Internet
Engineering staff have ssh access to the App Tier, which acts as Bastion
Authorized 3rd parties can be granted ssh access to select AWS resources, such as the Database Tier
All other Internet ports blocked by default
Amazon EC2 Security Group Firewall

Figure 4: Amazon EC2 Security Group Firewall

AWS Security regularly engages independent security firms to perform external vulnerability threat assessments.

Qu. Do you undertake any active vulnerability scanning of your internal infrastructure (e.g. Operating Systems, Databases, and Applications)? If yes, please give details including remediation.

AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities.

In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership.

In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment.

Qu. How is remote access securely managed? Who is granted remote access and how?

Graphical Data does not operate remote access method to it's internal network. Graphical Data uses the same Secure Socket Layer ©SSL® techniques to connect with AWS Data can therefore be transferred securely to and from AWS © including S3 and EC2 services. SSL is a cryptographic protocol designed to protect against eavesdropping tampering and message forgery.

Qu. Are operating systems, databases, and applications hardened to a standard build configuration?

Yes except operating systems on employee machines. Graphical Data adhere to best security practices when it comes to hardening our infrastructure.

Qu. What intrusion detection (IDS) / prevention (IPS) systems are installed and are they host and/or network based?

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics.

GD Internal hardware-based intrusion detection system employed in Internet access infrastructure described in point #6.1

Qu. What is your security patch management strategy? Please describe your approach and the controls applied.

- Security patches are applied depending on their purpose:
- external libraries used/linked are updated when their relevant patches become available and are approved by the library owner/community
- operating systems are updated as soon as a patch becomes available from the vendor (Mac OSX and Windows) otherwise subcomponents are updated daily (Linux)
- updates to GD software are developed and applied as soon as a vulnerability is found and a patch ready. Code security takes priority over functionality fixes.
- inventories are kept of all software and system components to compare the list of security patches installed on each system to the most recent vendor security patch list.
- We have a ranking system installed so the most critical, high risk vulnerabilities are addressed as highest priority.

Qu. What types of malicious code and malware detection software do you use? Where is it deployed and what is the update mechanism?

ClamAV is the software package used. It is deployed on:

- development servers used for code testing
- local machine used to access GD internal network
- Updates to threat signatures are downloaded daily and updates to the core AV solution are handled on when-available basis.

Qu. Does your organisation have a formal Change and Release Control process that requires approvals?

GD high level process for change management includes:

1. Identify and Raise Request for Change

2. Request is evaluated and assessed by appropriate personnel

3. Change is either rejected or authorised by the appropriate stakeholders.

4. If authorised, change will be implemented, tested, quality assured and released. We use pre-production environment which exactly replicate our productions systems to properly text before deployment.

Throughout the process all requests are recorded and stored.

AWS Change:

AWS applies a systematic approach to managing change so that changes to customer-impacting services are thoroughly reviewed, tested, approved, and well-communicated. The AWS change management process is designed to avoid unintended service disruptions and to maintain the integrity of service to the customer. Changes deployed into production environments are:

- Reviewed: Peer reviews of the technical aspects of a change are required.

- Tested: Changes being applied are tested to help ensure they will behave as expected and not adversely impact performance.

- Approved: All changes must be authorized in order to provide appropriate oversight and understanding of business impact.

Changes are typically pushed into production in a phased deployment starting with lowest impact areas. Deployments are tested on a single system and closely monitored so impacts can be evaluated. Service owners have a number of configurable metrics that measure the health of the service's upstream dependencies. These metrics are closely monitored with thresholds and alarming in place. Rollback procedures are documented in the Change Management (CM) ticket.

When possible, changes are scheduled during regular change windows. Emergency changes to production systems that require deviations from standard change management procedures are associated with an incident and are logged and approved as appropriate.

Periodically, AWS performs self-audits of changes to key services to monitor quality, maintain high standards, and facilitate continuous improvement of the change management process. Any exceptions are analyzed to determine the root cause, and appropriate actions are taken to bring the change into complain

Qu. Are changes and releases vetted for security vulnerabilities?

One of the steps involved during Change Request evaluation is to verify that no data, internal structure or protected piece of the architecture will be exposed if requested change were to be implemented. Failing to meet these criteria will cause the Change Request to be rejected and reasons for it communicated back to the party proposing the change.

Industry best practices are used in assessing security vulnerabilities, including OWASP.

Qu. Does your organisation have separate test and production environments?

Yes. Test/development environment is set up behind firewalls on an internal server accessible only internally in Graphical Data premises.

Qu. Is a security event management system in use, and is it operated in an effective manner?

AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business impacting events.

Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved.

Considering the current size of our company (GD), we do not currently feel SEM is required.

Access Control

Qu. Who will have access to client data (in all environments, e.g. test, UAT, production etc)? Please describe by function (vendors, customers, end customers, partners, operational support, developers etc.)

- Technical Director, developer, operational support
- Senior Developer
- operational support, data manager
- For up to date information please contact info@graphicaldata.co.uk

Qu. How will this access be audited?

All access records are stored in GD internal ticket tracking tool. Data access events are recorded and monitored

Qu. Will this audit data be available to client?

Yes if required

Qu. Does your organisation allow "all powerful" or high privileged accounts on the system? If yes, how many people hold such an account? How is this controlled? Please provide details.

GD systems are protected according to security best standards. Our engineers elevate privileges only temporarily for needed administrative tasks. No super-user logins are allowed on production systems, or those handling customer data, and that account is locked with an unknown value set as password. Only one other account is allowed to execute tasks with super-user permissions

Qu. Is there a formal process for granting, enabling, requesting, authorising, monitoring and deleting access to client data?

Lukasz Piwko, our technical director, will manage Access Control to any customer data. Considering the size of our organisation, we do not feel a complex process is necessary. GD do, however, have standards for maintaining the list of User Roles and Account profiles, processing access requests and ensuring all permissions and users are kept up to date.

Disaster Recovery

Qu. Please describe your disaster recovery procedure or processes:

These are the simplified steps of GD DR procedure:

1. In the event of the disaster being detected by GD we notify everyone who is affected and provide a channel (email address) of communication where further updates will be broadcasted.

2. Establish where the problem lies - hardware or software (or both).

3. Create a detailed procedure based on found facts geared toward reaching a resolution.

4. In case of hardware (networking also included) issues we push requests to AWS to look at the problem.

5. Software issues are put through our engineering team with a high priority on resolution immediately after such an issue is detected.

6. If a resolution is not expected to be provided in reasonable time we try to establish a working service using a secondary environment so that work interrupts are kept to a minimum.

7. After a resolution is reached we communicate our findings and final solution to relevant parties. Each incident is tracked along with its characteristics and regular analysis is performed to limit any further incidents from happening based on the same or associated criteria.

GD utilize various AWS features to create a DR environment, including:

- Storing DR back up facilities in a different region that main deployment.

- Amazon S3 storage facilities (objects stored on multiple devices across multiple facilities within a region, designed to provide a durability of 99.99999%).

- Amazon EC2 - Amazon Machine Images allow for preconfigured OS and application stacks, which can be launched as part of a DR procedure.

- Amazon Route 53 - DNS web service.

Qu. What are the recovery timescales?

Our recovery time would be no greater than 6 hours.

Qu. Has this process been tested recently (last 12 months)?

Yes, Annually – and successfully.

For most recent test date, please contact info@graphicaldata.co.uk

Technical / Operational Support

Qu. Please provide details (including internal and external Service Level Agreements) of the technical / operational support services available to your employees engaged in servicing the proposed contract

GD benefit from the SLA's provided by AWS as the Resolve platform sits on top of this service:

AWS EC2 SLA: http://aws.amazon.com/ec2/sla/

AWS S3 SLA: http://aws.amazon.com/s3/sla/

System Support is available during business hours (0900 - 1730). Specific SLA's are available to customers of the Resolve service upon request. Support can be requested via the Resolve front end or support request tickets can be raised through email. Staff are located in Belfast, UK.

Technical Asset / Infrastructure

See separate documentation on latest build and configuration.