Boomerang Triage
Service Definition
G-Cloud 11

Contents

1 Purpose

This document defines how Boomerang Triage is delivered to customers for the purposes of the G-Cloud service catalogue. It covers the following:

- An overview of the service provided
- The Platform infrastructure from a security and operational performance perspective, consisting of the:
    - Physical environment
    - Platform architecture
    - Service architecture
- Service implementation
- Service management
- Support services

2 Scope

This document defines the end-to-end delivery of the Boomerang Triage service and applies specifically to users of the G-Cloud service catalogue.

3 Definitions & Notes

3.1 Definitions / Acronyms

Acronym / Item	Definition
A2P	Application to Person
API	Application Programming Interface
Cascade	The sequence of communication methods, the order by which End User's receive these communications and the intervals between which each communication method is invoked – otherwise known as 'workflow'. Each cascade is automatically assigned a unique reference
CDMA	Code Division Multiple Access
CSV	Comma Separated Value
Destination Id	The End User's Id at which a message terminates e.g. an Email address or mobile number
End User	The recipient of communications from Boomalert
GUI	Generic / Graphical User Interface
GSM	Global System of Mobile Communications
Incident	An event which triggers a pre-defined cascade to initiate the communication process with End Users.
Originating Id	The originator used when delivering a message denoting where the message arrives 'From' e.g. a virtual number or Email address
SOAP	Simple Object Access Protocol
SMS	Short Messaging Service
SMTP	Simple Mail Transfer Protocol
Threading	The matching of multiple outbound communications to one or many End Users, with their associated responses
TLS	Transport Layer Security
Virtual Number	A Virtual Number is a telephone number without a directly-associated phone line. A Virtual number can be either a short or long number
VN	Virtual Number

3.2 Notes regarding use of this document

- This document references the following documents which are available on request from Boomerang:
    - Service Description*
    - User Guide for the User Interface*
    - Business Continuity Plan
    - Information Security Procedures
    - Terms and Conditions (also provided in the G-Cloud catalogue)
- Where a section of text is highlighted in blue and underlined a hyperlink to the relevant place in the document is provided. Select Ctrl and click the link to be directed to this location.

*These documents are provided during the customer on-boarding process.

4 Overview of the Boomerang Triage service for G-Cloud

Boomerang Triage delivers and automates compliant customer initiated interactions. It is a turnkey solution for customer facing organisations.

The software has been designed to help organisations carry out efficient and consistent communications through digital messaging, ensuring that auditable records of messages are kept.

5 Information Assurance

5.1 Overview of approach to information assurance

The organisation currently complies with a range of the requirements, policies and controls, including Cyber Essentials and a more comprehensive approach that maps to ISO 27001:2013, the international standard for information security. Our practices will also ensure compliance with the information security and privacy elements expressed in the EU General Data Protection Regulations.

The following ISO 27001: 2013 focused tools, policies and frameworks are either in place or in the process of being implemented including a statement of applicability and objectives for:

- An information security management system (ISMS) scope to include the organisation and its staff, the products available over G-Cloud, and relevant supply chain activity that either processes customer data or has some interaction around it e.g. development of the service

- A risk assessment of our and customer information & related information assets based around the confidentiality, integrity and availability of the information. This ensures that appropriate and proportionate controls are put in place, in line with Annex A of the standard, and following ISO 27002 code of practice.

- Regular staff awareness and training, including an HR security lifecycle that covers recruitment, induction, in life management and exit of staff or change of responsibilities

- Performance evaluation at regular intervals including reviews of policies, management reviews, internal and independent audits as well as processes & tools for corrective action and ongoing improvement

- Other policies and controls in line with ISO 27002 to address risks and requirements in the areas of:
  - Asset management
  - Access control
  - Cryptography
  - Physical and environmental security
  - Operations security
  - Communications security
  - System acquisition, development and maintenance
  - Supplier selection and management in life, including a robust segmented approach to supplier work based on the information assets the suppliers have access to in line with the risk assessment
  - Information security incident management (including readiness for EU GDPR)
  - Information security for business continuity planning and disaster recovery
  - Other compliance in line with applicable legislation, privacy and protection of personally identifiable information

Additional capability already invested in includes processes and tools for managing specific aspects of EU GDPR such as subject access requests (SAR), incidents that require notification to the Information Commissioner's Office and victims. In addition, the organisation has invested in capability for undertaking privacy impact assessments (PIA) and working in line with both EU GDPR and ISO 27001:2013 for information security in projects.

5.2 Cloud infrastructure

The application layer and messaging services are delivered via a scalable cloud based platform with high availability and reliability, whilst guaranteeing the integrity, confidentiality and availability of data across all platform components. This section covers:

- The physical environment supporting the platform
- The platform architecture
- The applications / Services

5.3 Physical environment

The primary and secondary data centres are UK bound (Manchester and London respectively). Data centre services are compliant with industry leading standards and accreditations for both data centres are described below.

Data Centre accreditation

Security management

Both data centres have been awarded the ISO 27001:2013 standard for security management. It specifies the requirements for establishing, implementing, operating, monitoring and maintaining a documented Information Security Management System within the context of an organisation's overall business risks. It also ensures best practice for security controls to protect information assets.

The European Code of Conduct

This is a voluntary code which promotes the adoption of energy-efficient best practices amongst data centre owners and operators.

Quality management

Both data centres have achieved the ISO 9001:2008 standard for business quality management. It is applied to the processes that create and control the products and services to ensure that the needs and expectations of customers are met. The standard demonstrates the existence of an effective quality management system that satisfies the rigours of an independent, external audit

Environmental Management

Both data centres have achieved certification to ISO 14001, the environmental management system standard. ISO 14001 is an internationally recognised accreditation for organisations that demonstrate superior environmental management. The certificate highlights on-going commitment to both maximise the energy efficiency of its existing data centre estate and develop innovative new facilities.

Occupational Health and Safety Management

Certification to OHSAS 18001, the assessment specification for occupational health and safety management systems demonstrates the leadership to reduce risk and create an injury-free environment.

Data centre security

Access

Access to data centres is rigorously controlled at the perimeter and building access points. Professional security staff operate on a 24x7 basis, with access to video surveillance and intrusion detection systems. Access to the data centres is only permitted for staff members that have a genuine business need and visitors are accompanied at all times by authorised personnel. Visitors must always carry identification and must provide the require authentication to gain access to different areas within the data centres. Access to the operations rooms is controlled by a physical access control mechanism.

Power

Each production server has a UPS installed to provide back-up power to protect against power failures or surges in supply. A generator is used to provide power to protect the operation of all equipment in the event of a mains power failure. Each UPS and the generator are tested every six months. All power points are raised to protect against failure in the event of flooding.

Environmental conditions

All rooms are fitted with smoke / fire detectors and fire extinguishing equipment that are set to operate automatically when the computer room is left unattended for long periods. All rooms contain an adequate air conditioning system to provide a stable operating environment to reduce the risk of service outages due to component failure.

Data

All storage media in the data centre (e.g. tapes and documentation) are stored securely when not in use. Magnetic media that is no longer required and which may contain confidential data is disposed of securely, i.e. all data is erased or the media is rendered inoperable.

Monitoring and management

Both internal and external monitoring is utilised within the datacentre facility to monitor all key elements of the network and physical presence. Internally Network Node is utilised to capture inbound traffic levels into our core data centre network switching, Network Node will monitor the flow of inbound traffic and alert via email and SMS in the event of a traffic anomaly. Subsequent network analysis is performed by Arbor, which in turn monitors the inbound network for any DDOS attacks to the core switching or any BGP issues.

5.4 Platform architecture and security

The services operate on an enterprise level, fault-tolerant, cloud based platform powered by VMware vCLOUD and is secured using a redundant pair of Cisco ASA firewalls in active / passive configuration. This configuration is replicated across our primary location (Manchester) and secondary location (London) with full and immediate failover provided in real time between the two locations.

Network architecture

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. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, are used to manage the flow of traffic.

In addition, network devices are in place that are dedicated to managing interfacing communications with Internet Service Providers (ISPs). A redundant connection to multiple communication services are used at each Internet-facing edge of the network. These connections each have dedicated network devices.

Entry points to both networks (Manchester and London) are provisioned with a 1G bit dedicated internet feed, located upstream across multiple network carriers, spanning the whole of the UK. This guarantees the optimum network level integrity and connectivity speeds for both customers and suppliers. The services are built around an assured data transport mechanism and aligned to HMG PSN strategy.

Network monitoring and protection

A wide variety of automated monitoring systems are utilised to provide a high level of service performance and availability. These monitoring tools are designed to detect unusual or unauthorized activities and conditions across 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 and extensively instrumented to monitor key operational metrics within the application. 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 with communication escalated across a team of engineers to ensure required personnel are always available to attend to any incidents.

Cloud solution architecture

The solution has been designed to handle both active / passive and active / active load balanced configurations and with the ability to automatically expand overall capacity to accommodate any dramatic surges in traffic.

Data spans both geographical sites in real time and any data changes to the primary location are also replicated to the secondary location. All data is backed up externally every three hours and as data is transparent between sites, there is no need to backup and restore data across locations in the event of a failover - data locking and consistency is handled within the vCLoud platform.

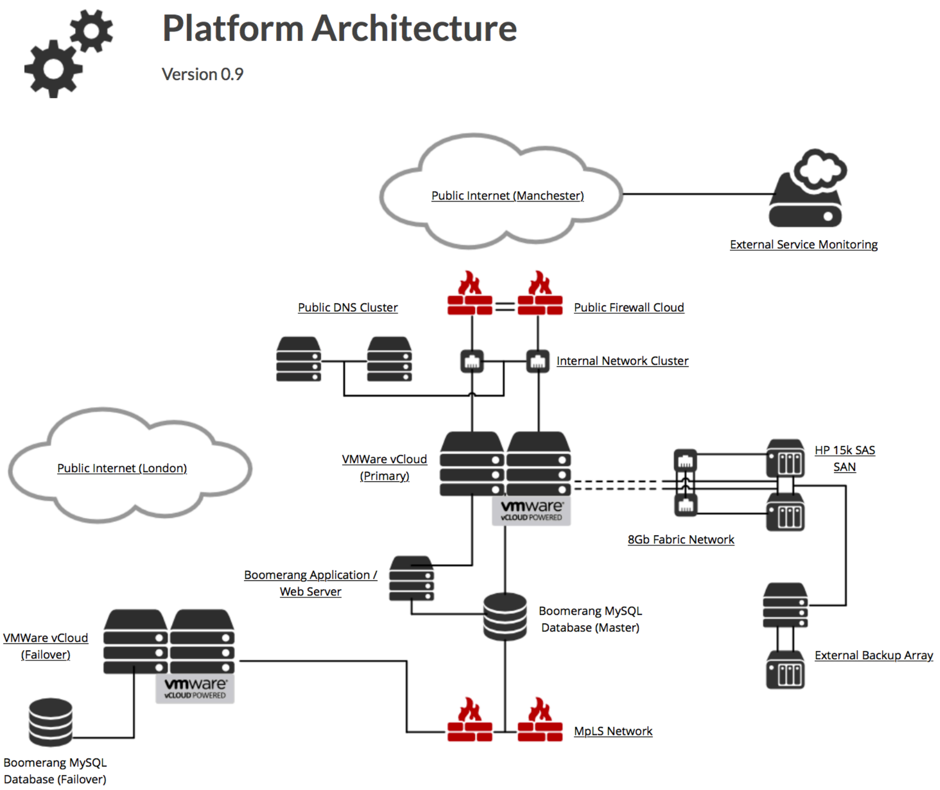

Figure 1 - Boomerang platform architecture

Cloud solution security

Internal connectivity to the platform is IPSEC secured directly by IP based firewall rules. This is also validated by regular scans carried out by an external provider checking the network tier and penetration of different components within the architecture. External access to the core cluster and application platform is permitted by a three-phase approach:

- Inbound connections are verified by the external firewall cluster and that will check to ensure the inbound connection has originated from a trusted IP address.
- Once the initial connection is made, the IP address is then verified by the internal firewall system
- Where access at the IP level is granted, then user-based authentication can take place.

IP access to the production platform is permitted by a strict change control process and revoked once access is no longer needed. User access is defined and SUDO permissions are granted again, based on a strict change control process that is regularly reviewed and approved internally. This level of control also makes it possible to permit access to individual tiers of the platform (the platform is split between web, application, database and audit logging).

5.5 Service architecture and security

Overview

The Services are configured on a LAMP stack – **L**inux, **A**pache, **M**ySQL, **P**HP, where Linux provides the core operating system, Apache the customer facing web services, PHP the core application code base and MySQL the database. These components are distributed across the Cloud.

The application layer includes all customer facing Services along with the message processor that is used process outbound message transactions, threaded responses and non-threaded inbound messages.

All components within the application layer have been configured to be modular, allowing each component to utilize its own hardware resources, whilst communicating securely with each other. Layering the architecture in this way allows each component to be independently secured using its own firewall and also provides the ability to readily upscale processing capacity against each specific component. This is represented in the diagram below

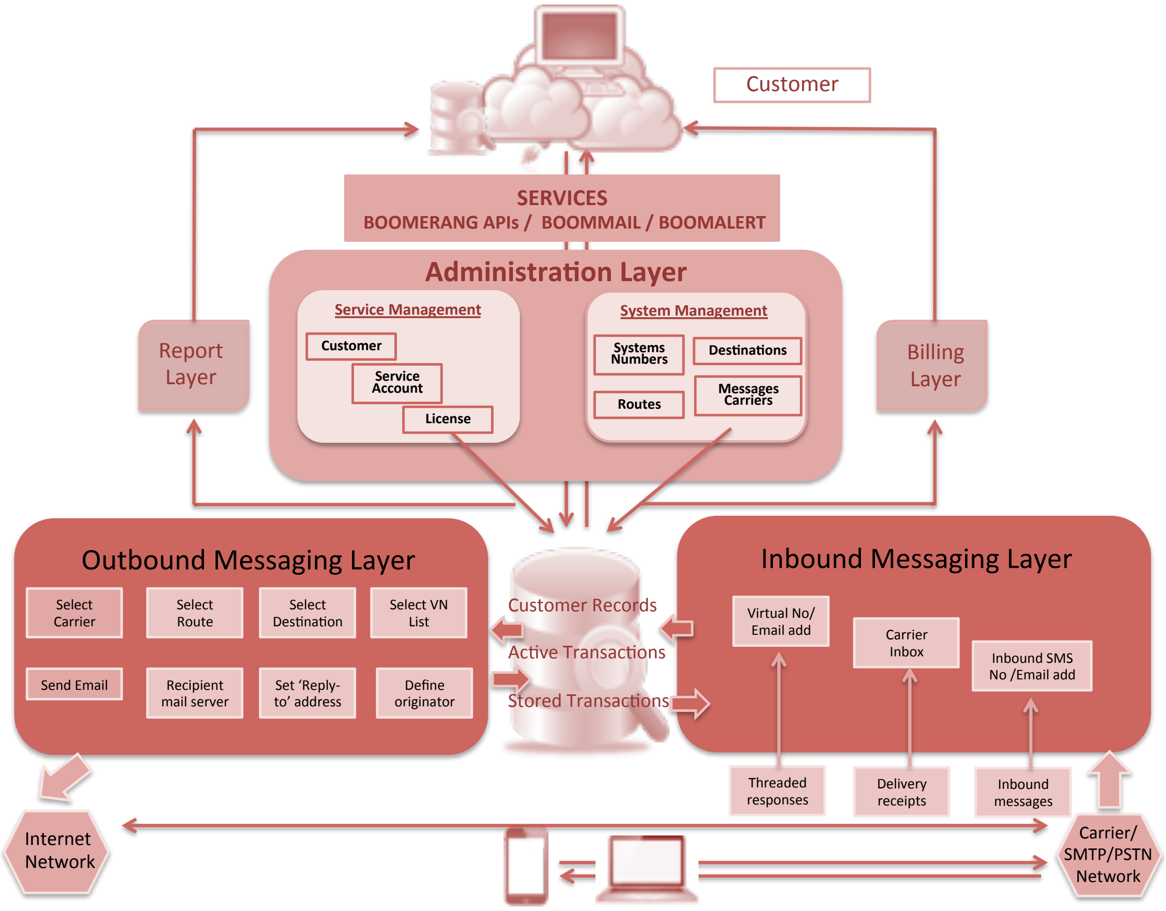

Figure 2 - Application layer

Secure access points

All Service access points (API endpoints and web browsers) are secured using SSL encryption (HTTPS), to protect against data interference. All data is encrypted from leaving the platform until received by the requesting device.

5.6 Data security across the platform

HR Security & User authentication

The requirements that safeguard the integrity and security of customer data are laid out in Security procedures and Company handbook, both of which are provided to all personnel. All staff with access to sensitive personal data are CRB checked prior to gaining access to any systems.

Access control procedures are in place that control how access to systems and network is allocated, revoked and periodically reviewed (aligned to our on / off boarding processes). Personnel are only provided with the required level of access to system data in order to fulfil their duties (‘least privilege’) and access is further controlled through the use of roles, permissions and login authentication. Access to systems is protected using rigorous password controls and all passwords are protected using cryptographic hash algorithms. Privileged access is managed by allocating user specific user IDs and the use generic user IDs is avoided. Controls are also in place to ensure that access to systems and network services is reviewed periodically by the system owner.

Key activities carried out by systems user are logged with the date and time the activity was performed.

Application data

Application data is segregated according to each Customer using a unique set of credentials that are required to access or retrieve it. The option for mobile number and message content to be entirely overwritten or partially obscured is provided, to prevent visibility of this data across any of the Service platform.

File storage and encryption

On and off-site backups are stored and encrypted to AES 256Bit Encryption. Access to the backup drives is only possible upon successful verification of the AES Private Key that is protected internally by relevant staff. The AES Encryption mechanism provides a further layer of data safety and protection to all backup data both on and offsite. The AES Key is changed every 12 months to ensure the upmost protection.

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. These procedures follow NIST 800-88 (“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.

Data retention policy

Data retention policies are aligned to industry and regulatory standards, including but not limited to the Data Protection Act 1998. Online personal data relating to message transactions is retained for 18 months for all transactions. Online data relating to stored recipients is retained for 12 months after off-boarding the Service Account. Back up data is retained for seven years unless otherwise specified.

Back-ups

Full daily level 0 backups are taken and held off-site using R1 CDP Data continuity. Backups are held on file for 365 Days and verified after each successful SNAP shot.

To compliment the daily backup set, hourly checkpoints are also taken and held on a rolling 30-day rotation. The backup set then allows the platform or specific subset of the infrastructure to be rolled forward / backward at any given time with no data loss. All system files and data are copied to a second storage node for redundancy and availability. Data is not backed up outside of the storage fabric and the user removes all copies upon expiration or deletion.

5.7 Malware prevention

Manual and automated scanners are used to search for websites that may be vehicles for malware or phishing.   We also use multiple anti-virus engines on servers and on workstations to help catch malware that may be missed by anti-virus signatures. Support team members are trained to identify and eradicate malware that might infect the network and unusual instances are escalated through the Operations team.

All production LINUX services are protected in real time using MALDET a LINUX malware protection service. In the event that any Malware is isolated on the production system, this is quickly quarantined, and alerts issued internally. MALDET performs a daily pattern update to which ensures that its internal scanning engine is kept up to date.

5.8 Platform monitoring and alarms

Externally the Service endpoints / APIs for both across the platform are monitored by IPPATROL from six different geographical locations, to ensure accuracy of monitoring.

An external monitoring application – Nagios is used to monitor the utilisation of resources across the platform:

- Availability of supplier URLs (a response is returned as part of the check)
- System users
- Number of connections used
- System load
- System Memory
- I/O Wait
- Disk usage
- Application queues (Gearman)
- Availability of Memcache
- MySQL load (simultaneous processes)
- Duration of MySQL queries

Each component that is monitored will trigger a Warning / Critical state alarm based on breaching pre-defined criteria. These metrics are reviewed quarterly to ensure their accuracy, relevance and reliability. An on-call schedule is used so personnel are always available to respond to operational issues with communication escalated across a team of engineers to ensure required personnel are always available to attend to any incidents.

5.9 Service availability – Business Continuity Management

The platform has been designed and built to achieve 5x9 service availability. VMware provides full hardware fault tolerance along with multi-site failover in the event of a Data Centre outage or network issue. Failover between data centres can be achieved within minutes to help minimize the impact of a site isolate disaster. In the event of an issue at the application level, we are able to roll back cluster instances in real time via SNAP shot that are maintained via our SAN architecture.

VMware configuration and managing node failure

Node failure does not impact the production platform as VMware fences the node and ejects this from the running cluster without service impact. Version 5 is currently used with 'DRS Configuration' post failover, along with the VMware Fault Tolerance module. This uses a VMware technology called LockSTEP which keeps a shadow copy (dual commit) of the running container mapped against the failover node. In the event of a failure on the primary node, the container continues to run without any loss of data or service, using its shadow copy to has a full map of the container's memory procedures and CPU calls. Operating a 10GBE network provides the shadow copy with rapid local interconnects.

Data replication between sites

All Services are replicated between sites, both memory and disk blocks are replicated in real time via VMware & SAN to SAN Replication. As such, when implementing a site failover, both memory and data is captured and replicated, thus removing any transition loss.

Live upgrade capability

The platform architecture enables live updates without the need for downtime. There is an Instant SNAP back capability in the event of an issue that is handled by VMware at our platform layer.

Service availability KPIs

Key performance Indicators are used to measure Service availability against pre-defined targets as below:

KPI Description	Measured
Service availability	IP Patrol monitoring
No. Of Service interruptions	Incident Log
Ave duration of interruptions	Incident Log
No. Of scheduled maintenance activities	Maintenance plan

A target value and an actual value are provided for each KPI item listed in the table above.

Business Continuity Plan

In addition to the redundancy of Services facilitated by the data centre architecture, a Business Continuity Plan is in place that defines how the organisation will continue to operate according to crises of varying severity. This plan is reviewed periodically and least once annually.

5.10 Change management

All changes are controlled and managed through a change management process that aims to minimise the impact of changes upon Service users. This process covers the following activities:

- Initiation and review of change requests
- Logging of all change requests
- Evaluation (of business impact and risk) and formal authorisation of change requests
- Drafting and approval of functional and non-functional requirements
- Design review
- Development of approved changes
- Testing of approved changes being applied
- Notification of scheduled release to relevant stakeholders
- Release of applied changes into production
- Post production evaluation and testing
- Applied changes and benefits notified to relevant stakeholders

Platform development and testing

Development practices are documented to ensure that the appropriate security and QA are considered and introduced at the requirements phase of all new development projects, prior to any development commencing.

All new development is carried out in a stand-alone development environment and developers follow coding guidelines (including OWASP) to ensure that application meets the required security standards. Code changes are 'peer' reviewed to provide additional validation and all code is commented with strict Change Control documentation used to define all changes in detail. A QA environment configured to replicate the development environment (which in turn replicates the production environment) is used to validate all changes.

QA Testing

QA testing consists of manual testing and automated using a set of pre-defined and approved test scripts. Full performance testing is carried out where applicable, to ensure that both reliability and efficiency of the Service are maintained prior to full deployment to production. Where necessitated by the changes made, full regression testing is carried out prior to full production deployment.

Service vulnerability QA

External tools are used regularly to ensure that security of the service is optimal and that industry standard best practices are continually adhered to:

- Vulnerability Management scans – Carried out against all assets in the Boomerang estate
- Web Application Scans – Checks and verifies that the application code is secure to DDS standards

Configuration updates

For OS and platform maintenance, updates to the cluster and OS platform are carried out quarterly or on an ad-hoc basis for urgent changes. This is to ensure that both cluster and operating systems are secure and up to date. Updates are performed out of hours and are performed with full roll back / SNAP shot in place. Cluster updates and patches at the OS level do not impact the Service or application as scheduled cluster maintenance can be performed off-line without any impact against the live Service, by means of VMware control. Any system configuration changes are first deployed in the QA environment for evaluation and risk assessment and all changes are recorded in the CMDB.

Change management KPIs

Key performance Indicators are used to measure change management activity against pre-defined targets as below:

KPI Description	Measured
Number of major changes (Annual)	Change log
Number of Emergency changes	Change log
Number of scheduled changes	Maintenance plan

A target value and an actual value are provided for each KPI item listed in the table above.

5.11 Scalability

The hardware supporting the Services is provisioned with resources that are managed by VMware and resources can be spread across the Cloud as and where required. The baseline resources provide substantial headroom to (automatically) accommodate dramatic spikes in messaging activity. The platform can provide 64 Physical CPU's at 2.4Ghz processing power and each CPU has 4 Cores. The platform SAN can provide 35,000 IOPS Disk I/O using the SSD Disk Pool with 284 GB RAM.

The messaging layer connects directly to the Boomerang messaging gateway (refer to Boomerang Messaging for more details) which has been designed to achieve substantial throughput across multiple messaging channels with the ability to manage sustained load over long periods. The existing configuration was designed to comfortably process several million transactions per day across working hours, without compromising processing capacity.

Scaling performance

As the application components are modular (allowing separate functional components to operate on their own hardware) the allocation of additional resources can be targeted to the specific areas required. For example, the interfaces to our message carriers could each run on independent hardware instances, allowing simultaneous connectivity to multiple carriers with multiple connections to each carrier.

From the infrastructure perspective, VMware Cloud Design allows the platform to scale without downtime or performance degradation linearly.   Cloud instances have been configured to use an auto-scale set of resource limits, within which additional resources are utilised as demand is increased. Furthermore, as end user demand grows, the VMware platform can provide an externally available VIP that can accommodate several customer facing web servers, thus providing a load balancing capability.

5.12 Incident responses

A documented Incident Management procedure is followed to manage any events that compromise the availability, performance or security of the service platform. The Operations team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. 24x7x365 coverage is provided to detect incidents, to manage the impact and facilitate a swift resolution. All incidents are recorded and assigned a severity level based on service impact and a root-cause investigation is undertaken culminating in a Root Cause Analysis (RCA) report to record the incident details and mitigation strategy.

Methods used to resolve an incident are logged in a Knowledge base and where applicable and the mitigating actions are formulated and implemented to prevent a recurrence of the same type of incident. We adopt a proactive approach to problem management by using trend analysis to prevent issues arising and to provide permanent solutions to known problems. All ‘problems’ are recorded and ordered according to priority (risk) and a strategy is developed to limit or eradicate the associated risk.

6 Customer on-boarding and off-boarding

The software is accessed via a cloud hosted web interface**.** This provides the ability to carry out the following:

- View a dashboard summary of system activity
- Manage system users and settings
- Import and configure system contacts and Groups
- Configure and manage Projects
- Build communication workflows – ‘Cascades’
- Trigger communication workflows
- Access incident reporting data and transactional messages reports

6.1 Trial customer on-boarding

To implement a trial service for a customer a request must be submitted via one of the following:

Email:	sales@boomcomms.com
Website:	http://www.Boomerangmessaging.com/trial
Telephone:	+44 (0)20 7224 5555

Profiling

On receipt of a request, a response is made within 24 hours to schedule a call with the customer to discuss requirements in greater detail, and to complete the ‘Customer implementation pro-forma’. This document allows intended usage to be profiled across the following criteria (if this information has not already been captured beforehand):

- The intended use case / cases and proposed workflow
- The communication channels required:
  - Email
  - SMS
  - Voice
- Message validity requirements
- Management of unmatched responses
- Management of all contact data (import / update)
- Account settings
  - IP restrictions
  - Warning periods (pre-purchased messages credits)
- Data security requirements
- Delivery destinations (by country)
- Approximate transaction volumes
  - Concatenated message volumes
  - Non-concatenated message volumes
- Training requirements

This call will also be used to ensure that all relevant contact details are provided. See below:

- An administrative contact – Responsible for overseeing day to day issues relating to the service
- A technical contact – Responsible for the implementation and ongoing maintenance of the service (e.g. recipient of planned maintenance notifications)
- A financial contact – Responsible for all financial matters relating to the account

Where it is not possible for the customer to provide all of the in the information required on the first ‘implementation’ call a further call will be scheduled for a later date.

User credentials

User credentials are provided to enable a primary contact to access to the user interface and consist of:

- **Username:** A username is unique for every account in the system.
- **Password:** A password must be at least 8 characters in length and consist of at least one upper and lower case character and at least one digit. The password requirements adhere to the requisite security standards

The primary user has the ability to create additional user accounts. Each additional user will receive an automated system generated Email containing user credentials and a link to the software.

The account will be configured according to the core requirements agreed on the ‘implementation’ call(s) and all relevant documentation is sent to the nominated contact. The documentation provided is listed below:

- Service Description
- User Guide

The trial account is active for 30 days from the point that the credentials and documentation are issued (this can be extended where agreed). 150 free message credits are provided automatically.

6.2 Live customer on-boarding

In addition to the process defined in the section above, the following go-live ‘gates’ must be completed and agreed with a customer wishing to proceed to a production service.

- Customer’s user testing has been completed and signed off
- Commercials have been finalised:
    - On-Boarding document completed: This document will provide a detailed breakdown of all service selections and their associated costs (where applicable) and will define any non-standard terms and conditions. The account will then be configured with the services, featured and settings defined in the on-boarding process
    - Purchase Order received: A valid purchase order must contain:
        - A Purchase Order number
        - Details of the services and featured being provided and all associated costs
        - Details to be used on invoices
- Any training agreed has been completed

- All customer roles / contact details have been provided
- The support model has been defined and agreed
- The 'Go-live' date has been confirmed and agreed

6.3 Customer off-boarding

Cancellation requests

All service cancellation requests must be submitted in writing and are subject to the cancellation period stated in the contract (standard 30 days). Where any additional services have been contracted to (dedicated or shared inbound short code services for example) the terms of these agreements will remain in place.

The service will remain active up to the agreed cancellation date and upon reaching the cancellation date, will be fully decommissioned and all subsequent requests to the service will be blocked. The customer will be obliged to pay any outstanding monies for subscriptions or message transactions that have not already been invoiced.

Requests for data

After a service has been decommissioned, a request to access data must be submitted in writing, specifying the data required and the timeframe over which it is required. The data listed below is available for extraction:

Message transactions

• End User's number
• Message content
• Content of response
• Source of the request
• Custom identifier

*End Users (recipients)**

• Name
• Email address
• Mobile number
• Landline number

*When adding End Users to the system it is possible to create 'User defined' fields in addition to those listed above. Any data added in 'User defined' fields can also be extracted.

System users

• Username
• Email address
• Password

Please note:

- During the customer on-boarding process, customers can specify elements of personal data that are to be automatically deleted on completion of a message transaction (e.g. mobile numbers or message content). Where this has been specified this data will not be available for reporting or billing purposes during an active service, nor will it be available for extraction after the service is decommissioned.

- A limit on the time period over which data extraction requests can be fulfilled (e.g. previous 6 months) may apply
- Requests for data would be completed within 48 hours working at no cost to the customer
- Upon completion of data extraction and after this has been provided to the customer, all transactional consumer data will be removed from all systems; including computers, storage devices and other storage media.

7 Service Management

7.1 Background and Overview

The Service has been designed to meet the following requirements:

- Support delivery of messages across the each of the available communications methods according to the required volumes.
- Provide access to a web hosted User Interface (GUI) facilitating the configuration and management of system data, cascades and Incidents.
- Provide delivery of messages containing across the specified communication method and with the relevant validity period.
- Provide support to the customer and actively participate in 2- way knowledge share.

The Service Model for our customers is grouped into Operational Services and Support Services as listed below:

- Operational Services
  - Multi-channel communication service
  - Account Administration
  - Reporting
- Support Services
  - Training
  - Operational Service Support
  - Account Management and reporting
  - Billing

7.2 Operational Services

Incident communication service

The service is fully defined in the document ‘Service Description’ which is available on request.

Account administration

Overview and Responsibilities

Boomerang will provide a user interface for the customer which will include the following:

- Provision and management of account settings
- Addition of services, products or features
- Amendment of existing service, product or feature selections
- Provision of ad-hoc message data on request

- Distribution of invoices and associated billing data

Support and Escalation

Any questions or issues surrounding account administration should be directed to the customer's System Administrator. If the System Administrator is unable to resolve the query, then the System Administrator can escalate it to the Technical Support team

Where still unresolved after the defined service level period, a query can be escalated from the System Administrator to the Head of Operations. Full details regarding the provision of support are contained within the Operational Service Support section of this document.

Reporting

SLA Reporting

Customers taking Boomcare Premium Support will be provided with reporting against Service Level Agreements upon a request being submitted to the Operations Team on support@boomcomms.com. This report will provide the following data:

- Service availability
- Response to service requests
- Service level 1 request solution timescale
- Service level 2 request solution timescale
- Service level 3 request solution timescale

Reporting provided in the user interface

The following reports will be accessible via the User interface:

- **Dashboard:** Provides overview of key system components using customisable 'widgets'
- **Live Incident reports:** This report provides a summary of the status of an incident:
    - Incident reference
    - Date / Time Incident initiated
    - How initiated and by who
        - System user details
        - Communication method
        - Mobile number
        - Email address
    - Total number of End Users sent to
    - Total number of End Users sent to by communication method
    - Total number of responses
    - Responses by communication method
- **Completed Incident reports:** As per the above report including a date and time of completion.

Aggregated totals are displayed along with the detailed transactional data relevant to each set of search criteria.

Reporting of message transactions

It is also possible to retrieve transactional message data in .csv format by sending a request to an SMTP reporting service. The request can be submitted from any email client and must contain valid account credentials along with the required start / end for the message transactions.

After validating the request an automated email is returned to the originator's email address with a .csv attachment containing all data.

Notes on reporting services

- The data returned will be 'as live' and will include any transactions up to the point that the request is submitted to the reporting service.
- Where a customer specifies any elements of data that are to be automatically deleted on completion of a transaction, these elements will not be included in any reports produced by the service.
- Data is returned for requests dating back no further than 3 months from the request date.
- Any requests that cannot be successfully validated will return an error message to the originator's email address. A user guide for the reporting service is also available on request from the Operations Team on support@boomcomms.com

Additional reporting requests

Consumer and crown level reporting data can be provided immediately on request based on the criteria listed on the table above.

Support and Escalation for reporting

If problems are encountered with the reporting service, the System Administrator can escalate such issues to the Operations Director.

Any queries arising that relate to the content of reports i.e. missing a SLA target or activity volumes that don't reconcile with the customer's systems can be escalated to the Account Manager.

7.3 Support Services

Training

Training Services

Training will be arranged by the customer's Account Manager and conducted by telephone. The customer will provide details of all attendees and will specify any particular items that should be covered. The session will provide an overview of the roles and requirements for the managed service, ensuring that the support and contact models are clearly outlined and will also address:

- Account configuration
- Overview of the multi-channel communication service
- User interface
- Reporting
- Billing
- Support services

Training Support and Escalation

Upon completion of training, any staff queries that arise from the training session should be initially directed to the System Administrator. In the event that such queries cannot be resolved by the System Administrator then the System Administrator can escalate to the support team.

Operational service support

Operational service support overview and responsibilities

The Operational Service comprises of:

- The message services
- Account administration.

Operational support will be provided consisting of:

- Service Requests
- Support Requests.

Service Requests

Service requests are raised and monitored through our Technical Support case management system. Such requests can be raised directly by the customer or by the Technical Support team at: technicalsupport@boomcomms.com. Each service request type is described below:

- **Customer originated requests**: Any customer representative raising a ticket is required to provide their name, e-mail address and a description of the request along with the priority level pertaining to nature of the ticket being raised. Confirmation of the service request, including a unique reference is sent to the e-mail address provided, with status updates issued as action is undertaken.
- **Support team request**: Where service requests are made verbally by a customer or internally to the Support team, a ticket is raised by the team using the method described above and confirmed to the nominated e-mail address also containing a unique reference.

All service requests are assigned a priority level ranging from one to three, where Priority 1 = Level 1 (High), Priority 2 = Level 2 (Medium) and Priority 3 = Level 3 (Low). Attributing the priority/severity of a request should be based on the definitions provided in the table below:

Support request type	Definition	Support contact	Escalation point
Level 1 – HIGH	The System is down and inoperable. All work has stopped and the situation is causing a critical impact to the Customers service. Examples: • A complete service outage • A recurring temporary outage of a critical service • Inability to provision a critical service • Substantial loss of billing data • Messages not received by the platform from the relevant Operator's network	Support team	Head of Operations

	• the platform unable to send messages to the relevant Operator’s network • Customers are unable to connect to the platform • Platform corrupts messages		
Level 2 - MEDIUM	System is severely limited or degraded. The situation is causing a significant impact to certain portions of the Customer’s service. The System is interrupted and recovered but has a high risk of reoccurrence) Examples: • Servers connected to some of the operators have traffic disturbances, however not all operators affected. • Significant degradation of a critical service occurs • Results of critical services are materially different from those described in the product definition		
Level 3 - LOW	Problems or disturbances affecting a specific area of functionality, but not the whole system. Serious disturbance with impact given to end-user services. Examples: • Congestion in the system causing the System to reject some messages. Degraded performance or incorrect behaviour of a specific area of functionality, but not the whole system. • General consultation and minor problems that have a minor effect on the functionality of the System. Problem encountered; irritant; minimal impact to business operation • Faults that do not disturb traffic or cause any loss of service such as incorrect System printouts, documentation faults, and minor design imperfections. Operational questions. • A small system delay occurred, but no loss of data is experienced • A minor application error occurred • Documentation errors.		

Severity Level 1 – High Priority Service Request (incl. unplanned outages)

Where a Level 1 severity support request is identified, the following course of action is undertaken:

- A notification will be sent by e-mail to all the customer, including all nominated customer contacts, the Operational Support team and Account Manager, along with all designated supplier contacts, containing:
  - A description of the fault
  - Expected timeframe for service interruption (if known)
- A progress update is sent to the customer every hour.
- A notification is sent to all stakeholders upon resumption of service
- A final notification will be sent to all stakeholders detailing the cause of the outage along with a summary of the resolution and a description of the measures taken to guard against any recurrence

Support Requests

Types of support request

The table below lists the different requests requiring reactive support. These requests should be received from the appropriate customer contact points, highlighted in the "Request initiation" column. All requests should be made in writing, providing a detailed description of the issue. All verbal requests should be supported by a written request and submitted within 30 minutes.

Support request type	Definition	Request Initiation	Support contact	Escalation point
"How to" queries	1. Service integration or service administration queries/requests	Customer's User	Customer's Relationship Manager	Support Team
Billing queries	1.Invoices/credits/statements 2. Payments 3. Billing information changes 4. Other	Financial Administrator	Accounts Dept	Operations Director
Service change requests	Service change requests	Customer's Relationship Manager	Account Manager	Operations Director

Support packages

There are two customer support packages:

- Boomcare Standard
- Boomcare Premium

The table below summarises the level of support applicable to each package:

Support element	Boomcare Standard Support	Boomcare Premium Support*
Support availability		
Support times	9am-6pm, Mon-Fri (UK)	24/7
Support channel	Email	Email, Telephone
System availability		
Target availability	No commitments	99.50%
Issue response times		
Severity level 1	24 hours	1 hour
Severity level 2	24 hours	1 hour
Severity level 3	24 hours	1 hour
Service Restoration Target		
Severity level 1	No commitments	3 hour fix time

Severity level 2	No commitments	5 hour fix time
Severity level 3	No commitments	2 day fix time
Scheduled Maintenance		
Notice period	5 days	5 days
Actions per month	No commitments	Maximum of 2
Terms		
Minimum term	N/A	12 months
Payment terms	N/A	12 months in advance

*Chargeable at contracted rate

Service Levels definitions and targets

	Service Item	Service Subcomponents	Service Description	Target SLA	Success Criteria
1	Service Availability	1.User Interface 2. API	Service Provision	99.50%*	No more than 223 minutes of accumulative recorded service disruption per calendar month.
2	Support	End Customer Response	Response Time to Email or call	1 Hour*	Customer support response should not exceed End Customer Response time.
3	Support	Fix Time Level 1	Critical Global Customer affecting issues. Both Service & Administrative functions.	3 hours total fix time. 2 hour customer update.*	Customer support response should not exceed defined Fix times based on support severity.
4	Support	Fix Time Level 2	Customer specific issue, affecting a single customer. If more than two customers report issue, this should be defined as a Level 1 Incident.	12 hour fix time. 4 hour customer updates.*	Customer support response should not exceed defined Fix times based on support severity.

5	Support	Fix Time Level 3	Specific customer function which does not impact on core customer end to end services.	2 day fix time. Notification to customer on completion*	Fix time should not exceed 2 days.

***These SLAs are only provided to customers with Boomcare Premium support**

SLA penalties and service credits

Boomcare Premium customers are entitled to Service Credits based on a failure to meet the monthly System Availability of 99.95%. Where Boomerang fails to meet this target in respect of any calendar month, subject to the paragraph below, Boomcare Premium customers will be entitled to claim a Service Credit of 10% of the monthly value of the service subscription paid in respect of the Service affected (being one twelfth of the total annual amount paid). Service Credits are not provided against any other annual or monthly charges (including but not limited to message credits) nor in respect of any other metrics or performance measurements.

To receive a Service Credit, the Customer must submit a claim by email to Boomerang at operations@boomcomms.com, including sufficient detail to allow Boomerang to validate the claim, within 30 days following the end of the month in respect of which the Service Credit is claimed. Service Credits will be applied at the end of the Initial Term for the Service, in respect of the Renewal Period and will not be exchanged for monetary compensation. The aggregate maximum Service Credits to be issued against all System Availability during any calendar year in respect of any Service shall not exceed 30% of the annual service subscription fees paid in respect of that Service.

A Customer is not entitled to Service Credits if it is in breach of its agreement with Boomerang, including without limitation where the Customer is not up-to-date with its payments when the relevant Outage occurred or Service Credits are claimed

Summary of Support contact points

Contact	Tel	URL / Email
Technical Support tickets	N/A	technicalsupport@boomcomms.com
Operational Support Team	+44 (0)20 7224 3333	support@boomcomms.com
Operations Director	+44 (0)20 7224 5555	operations@boomcomms.com

Account Management Service

Account Management Overview and Responsibilities

An Account Manager will oversee service implementation and support the ongoing development of the customer account. Acting as the primary point of contact for discussions around overall service performance the Account Manager will provide regular contact to discuss and analyse key metrics.

It is the responsibility of the Account Manager to:

- Schedule and coordinate the account management meetings / reviews
- Proactively deal with issues and concerns escalated by the customer Sponsor.

It is the responsibility of the customer's Sponsor to:

- Participate in the account management meetings / reviews.
- Proactively deal with issues and concerns escalated by the Account Manager.

Pre-Implementation Account Management

Your Account Manager will be available as required, during implementation. This will include regular contact by telephone and face to face meetings. The primary focus of the Account Manager during the course of implementation will involve:

- Finalising the contract and obtaining signatures
- Managing the scope of the contract and processing Change Requests / Variation Orders.
- Acting as the point of contact for the customer's Project team, participating in project governance activities as required.
- Establishing the relevant contacts for the customer across the following areas:
    - **Support Contact:** Responsible for overseeing the technical implementation and receives prior notifications concerning any planned or unplanned outages
    - **System Administrator:** Responsible for the day to day administration and account management
    - **Financial Administrator:** Responsible for all financial matters including receipt of invoices, credit notes and account statements.

There are no contractual Service Level Agreements (SLA's) in place for the Account Management service.

Post implementation Account Management

The Account Management model will need to be agreed with the customer but the standard model is defined below:

The primary focus of the Account Manager post-implementation will involve:

- A post implementation courtesy call addressing any questions or issues that may have arisen that week or remain unresolved by the Support Team. Thereafter:
- Quarterly review meetings (by conference call unless a face-2-face meeting is requested) providing:
    - Review of the service performance i.e. volumes sent, volumes received
        - Analysis of service performance against SLA's (for customers taking Boomcare Premium support)
        - Assessment of existing requirements and further expectations
        - Review of the commercial status e.g. billing and any outstanding payments
    - Executing post-launch PR activities as agreed with the customer.

Account Management Reporting

The account manager is responsible for reporting:

- Minutes and actions arising out of the monthly review meetings
- The end of contract 'value report' stating benefits derived by the customer from the delivery of the service.

Billing

The customer will provide a purchase order (including a valid purchase order number) which will specify the following:

- The service subscription required
- The message validity period required
- Any other fixed services that are required and defined in the on-boarding document
- The cost per outbound message
- Any other message costs that are required and defined in the on-boarding document
- The details required for the invoice

Any additional service features that are required after the initial account configuration must be purchased using a separate purchase order.

An invoice covering the annual subscription for the service is issued automatically upon account creation which requires payment within 30 days of issue. Thereafter, invoices will be provided on a monthly basis and issued to designated billing contacts on or around the first of each month. As part of the standard billing model:

- All service subscriptions are charged annually in advance
- Messages are billed monthly in arrears
- All invoices will include a breakdown of message activity and the associated costs by country
- Where a customer specifies any elements of data that are to be automatically deleted on completion of a transaction, these elements will not be included in any reports produced by the service.

Any deviation from this model must be agreed by Boomerang and included in the customer agreement, in the section for non-standard terms and conditions.

All billing documentation is provided in PDF format and will contain a summary of all message traffic to have passed through the account, broken down by country along with any fixed subscription charges associated to the account.

Any billing queries must be directed to billing@boomcomms.com and should also be issued in writing within 20 days of the invoice date. Any unresolved billing queries should then be directed to the Operations Director.

There are no contractual Service Level Agreements (SLA's) in place for the billing service.

8 Consumer responsibilities

Consumer responsibilities are covered in the Service Management section of this document and also in Customer's Obligations' of the 'Terms and Conditions' which defines the consumer's obligations in full. These terms and conditions are also available in the G-Cloud catalogue.

9 Technical requirements

This section defines the pre-requisites for integration.

9.1 User interface

The User Interface is accessed from a web browser via an SSL secured URL. All mainstream web browsers are supported and details of the version supported for each type of browser are provided in the technical documentation. Some customers may require training on certain aspects of the functionality, in particular the configuration of workflow processes. This can be arranged on request.

10 Trial Services

30-day trial access to the Service is provided which includes an allocation of 150 message credits. The trial service includes all functionality that will be available in the production version of the software (access to certain functionality may depend on the type of service purchased in for production). The trial is subject to the standard terms and conditions which are provided in the G-Cloud catalogue.

11 Termination terms and service migration

11.1 Termination terms

Consumer termination terms

Customer termination terms are set out in the 'Termination' section of the terms and conditions which are provided in the G-Cloud catalogue.

Supplier termination terms

All trial customer and production customers will receive 90 days' notice of removal of services from G-Cloud. Where services are withdrawn from G-Cloud, existing agreements will be honoured.

11.2 Service Migration

This information is covered in the section entitled 'Customer off-boarding' earlier in this document.

.