

Boomerang Service Definition For G-Cloud 15

Version	1.0
Date	9th January 2026

Contents

1 Company 9

2 Overview 9

3 Document Purpose 9

4 Overview of G-Cloud 15 Services Provided by Boomerang 10

4.1 CPaaS Messaging & Workflow Platform 10

4.2 Broadcast Messaging 12

4.3 API Messaging - boomAPI 13

4.4 Microsoft Messaging 15

4.5 Email-to-SMS and Email-to-Voice Messaging 19

4.6 Inbound Communications 20

4.7 Monitoring & Alerting 22

4.8 Logic Solutions 24

4.9 AI Services 25

5 Approach to Information Assurance 27

5.1 Overview 27

5.2 Information Security Management System (ISMS) 27

6 Business Continuity Management and Disaster Recovery Provision 29

6.1 Business Continuity Management 29

6.2 Service Resilience and Architecture 29

6.3 Backup and Data Recovery 30

6.4 Monitoring and Capacity Management 30

6.5 Change and Maintenance Resilience 31

6.6 Disaster Recovery 31

6.7 Testing and Continuous Improvement 31

6.8 Buyer Assurance 31

7 Securing the services 32

7.1 Network security 32

7.2 Cloud and platform security 32

7.3 Application security 33

7.4 Malware prevention 33

7.5 Security and vulnerability testing 33

7.6 Securing data 34

7.7 Access controls 34

7.8 Staff recruitment and training 35
7.9 Data retention and legislative compliance 35
8 Customer On-Boarding & Off-Boarding 35
8.1 On-Boarding 35
8.2 Off-Boarding 36
9 Service Management 36
9.1 Background and Overview 36
9.2 Operational Services 37
9.3 Training services 37
9.4 Service Constraints and Maintenance 37
9.5 Operational service support 38
9.6 Support packages 38
9.7 SLA penalties and service credits 39
9.8 Account Management Service 39
10 Customer requirements & Technical Pre-requisites 40
10.1 Customer requirements 40
10.2 Technical pre-requisites 40
10.3 Service Constraints 41
Appendix A - Functional specification for Boomerang CPaaS Messaging & Workflow Platform 43
1 Overview of CPaaS Messaging & Workflow Platform 43
1.1 Platform Capabilities 43
2 Logic Workflow Engine 44
2.1 Overview 44
2.2 Communication Channels 45
2.3 Messaging Solutions 45
2.4 Workflow Engine Overview 46
2.5 Workflow Architecture 46
2.6 Workflow Activation 46
2.7 Workflow Components 48
2.8 Integration & Extensibility 51
2.9 Security, Governance & Access Control 51
2.10 Non-Functional Considerations 51
3 boomLogic API Connections 51
3.1 Overview 51

3.2 Core API Connection Functionality 52
3.3 Supported API Connection Types 52
3.4 Third-Party API Connections 54
3.5 Nylas Integration 56
3.6 Messaging / Direct API Connections 57
3.7 Common Metadata Fields 57
3.8 API Lifecycle Management (Create, Update, Delete) 58
3.9 Security and Credential Handling (Where Applicable) 58
3.10 Status and Environment Control 58
3.11 Monitoring, Logging, and “Last Used” Tracking 58
3.12 Client and Ownership Validation 59
4 Asset Management 59
4.1 Overview / Purpose 59
4.2 Key features 59
4.3 Asset information 59
4.4 Managing Assets 60
4.5 Location tracking 60
4.6 Assigning Contacts 60
4.7 Asset hierarchies 60
4.8 Searching, filtering and listing 60
4.9 Summary information 61
4.10 Benefits for public sector organisations 61
5 Monitoring 61
5.1 Overview 61
5.2 What the service does 61
5.3 Monitor types 62
5.4 Key features 62
5.5 Security and data protection 63
5.6 Data handling and persistence 64
5.7 Standards and formats 64
5.8 Service limitations 64
5.9 Service management and support 64
5.10 Integrating Monitoring with Logic Workflows 64
6 Events 66

6.1 Overview 66
6.2 Creating an Event Manually 66
6.3 Automated Events 67
6.4 Event management and updates 68
6.5 Stakeholder interactions 68
6.6 Incident timeline and audit trail 69
6.7 Ticketing and event correlation 69
6.8 Access control 69
7 Reporting & Dashboards 69
7.1 Overview 69
7.2 Types of Reporting Data 70
8 Broadcast Messaging Interface 71
9 Messaging API 71
10 Email-to-SMS and Voice 72
11 Inbound Communications 72
Appendix A – Schedule 1: Workflow Actions Reference 72
1 Overview 72
2 Actions Defined 73
Appendix A – Schedule 2: Workflow Conditions Reference 79
1 Overview 79
2 Conditions Defined 79
Appendix B - Functional specification for Broadcast Messaging 84
1 Overview 84
2 Core Messaging Capabilities 84
2.1 Multi-Channel Messaging 84
2.2 Channel-Specific Message Variants 84
2.3 Channel Selection and Delivery Rules 84
2.4 Consistent Personalisation Across Channels 85
2.5 One-Way and Two-Way Communication 85
2.6 Scheduling Broadcast Sends 87
2.7 Example Use Cases 87
3 Message Templates and Ad-Hoc Sends 87
3.1 Template mode 87
3.2 Ad-hoc send mode 88

4 Rich Content and Editor Support 88
4.1 Overview 88
4.2 Rich Text Editing 88
4.3 Channel-Appropriate Rendering 88
4.4 Short Links and Controlled Access 89
4.5 Tokens and Personalisation 89
4.6 Preview Before Sending 89
4.7 Separation of Editing and Sending 90
4.8 Consistent Rendering at Scale 90
4.9 Accessibility and Content Quality 90
4.10 Example Use Cases 90
5 Recipient Management 90
5.1 Dynamic Grouping of Contacts 91
5.2 Contact Lists 92
5.3 File Import for Bulk Sends 93
6 Auditability and Metadata 94
6.1 What Is Recorded 94
Appendix C – Functional Specification for API Messaging 96
1 Overview 96
Appendix D – Functional Specification for Microsoft Messaging 97
1 Overview 97
1.1 Microsoft Custom Connector 97
1.2 Dynamics 365 Messaging Plug-In 97
Appendix E – Functional specification for Email-to-SMS and Email-to-Voice Messaging 98
1 Overview 98
2 Access 98
3 Communication Channels 98
4 Messaging Solutions 98
5 Messaging features 98
6 Service management 99
7 Reporting 99
7.1 Dashboard View 99
7.2 Transaction Reporting 99
Appendix F – Specification for Inbound Communications 101

1 Service Overview 101
2 What the Service Does 101
3 Supported Channels 101
4 Inbound Message Model 101
4.1 Attachments 102
5 Handler Configuration and Matching 102
5.1 Handlers 102
6 Matching Logic 102
6.1 Processing After Matching 103
6.2 Inbound Handler Actions 103
7 Reporting and Search 104
7.1 Inbound Statistics 104
8 Common Use Cases 105
Appendix G – Functional Specification for Monitoring & Alerting Service 106
1 Overview 106
2 What the service does 106
2.1 Monitor types 106
2.2 Key features 107
2.3 Status and lifecycle 108
2.4 Triggers and automation 108
3 Alerting workflows and communication management 108
3.1 Workflow capabilities 108
4 System Event Management 108
5 Security and data protection 109
6 Data handling and persistence 109
6.1 Creation and updates 109
6.2 Deletion 109
6.3 Standards and formats 109
7 Service limitations 109
8 Service management and support 109
8.1 Monitoring visibility 109
9 Typical use cases 110
9.1 Automated incident alerting 110
9.2 Recovery confirmation 110

9.3 Policy-driven communications 110
Appendix H – Functional Specification for Logic Solutions 111
1 Overview 111
2 Solution Catalogue 111
3 Functional Capabilities 111
4 Delivery Models 112
4.1 API-Integrated Solutions 112
4.2 User Interface-Driven Solutions 113
5 Workflow Configuration and Governance 113
6 Channels and Communications 113
7 Reporting and Insights 114
8 Commercial Model 114
9 Suitability for G-Cloud Customers 114
Appendix I – Specification for AI Services 115
1 Overview 115
2 Purpose of AI Processing 115
3 Scope of AI Capabilities 115
4 AI Functional Capabilities 115
5 Service Interfaces 116
6 Governance, Controls, and Safety 116
7 Data Handling and Compliance 116
8 Account and Service Models 116
9 Reporting and Transparency 116
10 Summary 117

1 Company

Boomerang I-Comms Ltd is a proven digital communications specialist, supporting UK public sector and international government organisations to deliver secure, reliable and inclusive messaging services at scale. With almost 20 years' experience, we specialise in high-quality 1-way, 2-way and intelligent 2-way digital messaging and communication workflow solutions across multiple channels, helping public bodies engage effectively with citizens, service users and staff. Our cloud-based solutions are designed to meet public sector end-to-end communication requirements, enabling automation of routine interactions, improved service accessibility through channel choice, increased operational efficiency, and enhanced citizen satisfaction through simple, frictionless and responsive digital engagement.

2 Overview

Boomerang offers a range of messaging solutions via an intuitive user interface and APIs that fulfil a broad range of messaging requirements. Our objective is to help organisations extend automation across customer and stakeholder engagements. Our 'Intelligent' conversation threading technology is unique and patented in over 50 countries and is pivotal to the products and services we deliver to our customers. Fundamentally, it addresses the core problems that have prevented true automation of business communications.

3 Document Purpose

This Service Definition describes the Boomerang Services made available via G-Cloud 15 and how these services are delivered to customers. The main body of the document provides an overview of Boomerang's G-Cloud 15 service portfolio and sets out Boomerang's approach to service provision and service management that underpins all services offered. Detailed specifications for each individual service available on the Boomerang G-Cloud 15 platform are provided in the appendices, structured as follows:

- Appendix A - CPaaS Messaging & Workflow Platform
- Appendix B – Broadcast Messaging
- Appendix C – API Messaging
- Appendix D – Microsoft Messaging
- Appendix E – Email-2-SMS and Voice Messaging
- Appendix F – Inbound Communications & Campaign
- Appendix G – Monitoring & Alerting
- Appendix H – Logic Solutions
- Appendix I – Boomerang AI Services

This structure aligns with the service overview and appendices described in the Service Definition document.

4 Overview of G-Cloud 15 Services Provided by Boomerang

Our comprehensive range of cutting-edge solutions empower organisations to fulfil their communication requirements from a single platform. A detailed specification for each solution is provided in the appendices to this document and summarised below.

4.1 CPaaS Messaging & Workflow Platform

Our CPaaS Messaging & Workflow Platform delivers a comprehensive, scalable foundation for building, orchestrating, and managing intelligent customer communications across channels and systems, providing customers with access to our entire suite of messaging services and solutions. Services can be accessed via user interface, APIs and Email client.

Features

Single unified messaging interface and extensive suite of messaging solutions A single, cloud-based platform provides access to all messaging, workflow, monitoring, and automation capabilities, supported by shared governance controls such as role-based permissions, audit logging, and central template libraries

Multi-channel messaging: SMS, voice, email, WhatsApp, RCS and Web Forms - The platform supports multi-channel communications including SMS, email, voice (TTS and calls), WhatsApp, RCS, and web links/forms, with configurable channel selection, fallback, and escalation.

Configurable workflows for automated business logic - Configurable workflows support broadcast and reply handling, time-based orchestration, conditions, actions, and integrations, enabling automation of complex business logic without bespoke development.

Real-time monitoring with alerting and escalation - Built-in monitoring and dashboards provide visibility into delivery success, workflow performance, and SLA indicators, supporting operational oversight and issue escalation.

Ready-made APIs for system integration - Standard APIs allow external systems to send, receive, and manage messages and workflows programmatically, enabling integration with existing digital services and applications.

Omni-channel messaging APIs for broadcast and conversational messaging -APIs support both one-way and two-way messaging across supported channels, enabling broadcast notifications and conversational interactions driven by external systems.

Broadcast messaging interface for high-volume, bi-directional messaging campaigns - A dedicated broadcast messaging capability supports high-volume outbound campaigns with optional reply handling, where responses are captured and processed by workflows.

Email-to-SMS and email-to-voice messaging solution - Email-triggered messaging converts emails into SMS or voice messages, allowing organisations to extend communications without modifying existing email-based systems.

Secure cloud hosting with role-based access controls - The service is securely cloud-hosted with role-based permissions, audit logging, and customer-specific policies for content, data handling, and access control.

Real-time delivery status tracking and reporting - Reporting and dashboards provide real-time visibility of delivery success rates, response metrics, workflow outcomes, and compliance indicators.

Benefits

Simplify messaging operations and reduce tool switching - By consolidating messaging, workflows, monitoring, and reporting into a single platform, users can manage all communications from one interface. This reduces operational complexity, shortens training time, and lowers the risk of errors caused by switching between multiple tools or systems.

Optimise reach across preferred user channels - Supporting multiple communication channels allows organisations to reach users through the channels they are most likely to engage with. This improves response rates, ensures critical messages are received, and increases inclusivity by accommodating different user preferences and accessibility needs.

Reduce manual operations and improve process consistency - Automated workflows replace repetitive manual tasks with repeatable, rules-based processes. This improves consistency, reduces human error, and frees staff time for higher-value activities, while ensuring communications are delivered in line with defined business rules.

Enable rapid detection and resolution of incidents - Real-time monitoring and alerting provide immediate visibility of delivery issues or service degradation. This allows operational teams to respond quickly, minimise disruption, and maintain service continuity, supporting SLA and operational performance requirements.

Accelerate integration with existing digital services - Ready-made APIs reduce the time and cost required to integrate messaging into existing systems. This enables organisations to extend current digital services with messaging capabilities without significant redevelopment, accelerating time to value.

Scalable automated communications across multiple channels from existing systems - Omni-channel APIs allow existing systems to trigger both broadcast and conversational messaging at scale. This supports high-volume, automated communications while maintaining consistent logic, tracking, and governance across channels.

Create scalable, interactive campaigns from an intuitive web interface - The broadcast messaging interface enables non-technical users to launch and manage high-volume campaigns with two-way engagement. Responses can be captured, tracked, and routed automatically, supporting surveys, notifications, and information requests at scale.

Extend email workflows to SMS and voice channels - Email-to-SMS and email-to-voice capabilities allow organisations to enhance legacy or email-based processes without system changes. This increases message visibility and urgency, particularly for time-critical communications.

Maintain secure, compliant communications aligned with public-sector standards - Secure cloud hosting with role-based access controls helps protect sensitive data and ensures only authorised users can access specific functionality. This supports governance, auditability, and compliance with public-sector security expectations.

Track message delivery to support audit, assurance, and reporting requirements - Real-time delivery tracking and reporting provide evidence that messages were sent, delivered, and responded to. This supports audit trails, performance reporting, service evaluation, and continuous improvement activities

A full specification for the Logic Workflow Engine is available in Appendix A.

4.2 Broadcast Messaging

Broadcast Messaging is a secure, multi-channel service for designing and delivering high-volume communications to large or targeted audiences. It supports SMS, email, voice, RCS and WhatsApp from a single interface, with reusable templates, personalisation, scheduling and delivery tracking. Broadcast enables both one-way notifications and two-way conversations, creating individual conversation threads per recipient. Designed for regulated environments, it provides role-based access and permissions, client isolation, validation, and comprehensive audit records to support transparency, assurance and compliance.

Features

Secure multi-channel messaging (SMS, Email, Voice, RCS, WhatsApp)
Supports outbound and inbound messaging across multiple communication channels.

Single broadcast interface with reusable templates
Provides a project-agnostic, modular broadcast service with reusable message templates.

Channel-specific message variants
Allows separate message content, formatting, and sender details per channel.

High-volume, regulated-environment support
Designed for high-volume usage with client isolation, permissions, and validation controls.

Dynamic audience targeting and recipient management
Supports targeted broadcasts using recipient data and configurable audience definitions

Personalisation with token validation
Enables personalised messaging using recipient data with validation before sending.

One-way and two-way messaging with response handling
Supports notifications and interactive conversations with reply processing.

Configurable handlers for delivery receipts and replies
Processes delivery statuses and responses through workflows, integrations, and reporting.

Flexible scheduling (one-off, recurring, event-driven)
Supports immediate, scheduled, and workflow-triggered message delivery.

Comprehensive auditability and delivery reporting
Provides delivery tracking, response outcomes, audit logs, and reporting dashboards

Benefits

Ensures reliable delivery across the most effective channels for recipients
Channel selection and fallback improve reach and message success rates.

Reduces effort and speeds delivery of repeat communications
Reusable templates minimise duplication and simplify broadcast creation.

Improves clarity and engagement by tailoring content per channel
Channel-appropriate formatting increases message relevance and usability.

Enables safe, compliant communications at scale
Governance, validation, and isolation controls support regulated environments.

Ensures messages reach the correct, up-to-date audience
Targeted recipient selection reduces mis-delivery and manual list maintenance.

Delivers accurate, consistent personalised messages at scale
Token validation prevents missing or incorrect personalisation data.

Supports both notifications and interactive engagement
Enables confirmation, feedback, and conversational messaging use cases.

Automates follow-ups, escalation, and system integrations
Handlers reduce manual intervention and enable downstream automation.

Ensures timely, reliable communications without manual intervention
Scheduling supports operational, regulatory, and service-driven timing needs.

Provides evidence for compliance, assurance, and service improvement
Audit records and reporting support transparency and accountability.

A full specification for Broadcast Messaging is available in Appendix B.

4.3 API Messaging - boomAPI

Boomerang's RESTful API delivers an ideal blend of security, functionality, and performance. Offering substantial throughput, it has been designed to meet the needs of enterprise customers requiring instant delivery of omni-channel messaging. The service is fully redundant, supported by a co-located infrastructure and premium connections to Tier 1 carriers, with automated failover inherent to both. It also provides access the next generation of conversational messaging using Boomerang's built-in intelligence guarantees that all messages and responses are matched across concurrent conversation threads. This empowers developers with the ability to build fully automated workflows from business applications.

Features

Multi-Channel Messaging
Supports Email, SMS (one-way, two-way, custom number), Voice (TTS), RCS, WhatsApp and Masked 2-way SMS.

Two-Way & Conversational Messaging
Enables full reply handling via SMS 2-way, email replies, inbound messages, and conversation threading.

Delivery Receipts (DRs) Retrieval
Provides detailed delivery status updates with paging, filtering, and deduplication support.

Inbound Communications
Allows retrieval of end use initiated inbound SMS messages by date, sender, recipient, or reference ID.

Conversation & Ticket Management
Supports open/closed tickets, conversation IDs, validity periods, and response tracking.

Short-Link Management
Automatically converts URLs into trackable short-links with expiry dates, visit limits, and password protection.

Masked Two-Way SMS
Enables anonymous, privacy-preserving conversations with configurable interaction limits and validity.

Social Hours & Time-Zone Control
Restricts message delivery to defined business hours using recipient location, time zones, or UTC offsets.

Campaign & Custom Metadata Support
Allows tagging messages with campaign names, custom parameters, and unique identifiers for reporting and tracking.

Delivery Priority & Scheduling
Supports message prioritisation and delayed delivery to control timing and urgency.

Benefits

Unified Communication Platform
Integrate email, SMS, and voice messaging through a single, consistent API.

Improved Customer Engagement
Two-way and conversational messaging enable real interaction, not just notifications.

Full Message Traceability
Delivery receipts, inbound replies, and transaction IDs provide complete auditability.

Scalable for High-Volume Messaging
Supports bulk messaging to up to 10,000 recipients per request.

Enhanced Privacy & Compliance
Masked 2-way SMS protects personal contact details and supports data-protection requirements.

Higher Conversion & Click-Through Rates
Short-links with tracking and expiry improve engagement while providing actionable insights.

Reduced Operational Overhead
Automated reply handling, callbacks, and reporting minimise manual processing.

Better Timing & Deliverability
Social Hours, priority flags, and scheduling help ensure messages are sent at the right time.

Flexible Integration Options
Simple REST endpoints with standard HTTP Basic Authentication allow fast system integration.

Actionable Reporting & Insights
Campaign grouping, response retrieval, and link analytics enable data-driven decision-making.

A full specification for API Messaging is available in Appendix C.

4.4 Microsoft Messaging

Microsoft Custom Connector

Boomerang's custom connector allows organisations to build intelligent messaging solutions from a range of services within Microsoft's Power Platform. The connector exposes Boomerang's omni-channel, Intelligent Messaging solutions to Microsoft Power Automate, Microsoft Power Apps, and Azure Logic Apps. It is the ideal solution for organisations looking to build 1-way or 2-way broadcast messaging, or automated conversational stakeholder engagements, from existing Microsoft applications such as Dynamics 365 CRM, ERP, plus applications with existing connectors such as Azure, IoT Central and Microsoft Teams.

Features

Multi-channel messaging support
Supports Email, SMS (one-way and two-way), Voice (TTS), and Push messaging within a single platform.

Intelligent two-way / conversational messaging
Enables replies to be tracked and mapped directly to outbound messages, supporting full conversations.

Response-driven automated workflows
Communication workflows dynamically adapt based on recipient responses, enabling true interaction.

Integration with Microsoft Power Platform
Available as a connector for Power Apps, Power Automate, Logic Apps, and Copilot Studio.

Bulk and individual message delivery
Supports sending messages to single recipients or large recipient lists.

Delivery confirmation and inbound response triggers
Provides triggers for delivery status updates and SMS response submissions.

Low-code / no-code enablement
Allows business users to build communication workflows without bespoke development.

Workflow automation and orchestration
Integrates messaging directly into business processes to automate tasks and decisions.

Global reach across geographies and languages
Designed for immediate communications across a vast set of locations worldwide.

Secure, authenticated API access
Uses authenticated connections to protect messaging transactions and data.

Benefits

Unified multi-channel communications
Engage users across Email, SMS (one-way and two-way), Voice, and Push messaging from a single connector, reducing complexity and ensuring a consistent communication experience.

Intelligent two-way conversations
Enable fully interactive messaging where replies are tracked and linked to outbound messages, supporting complete, auditable conversations.

Response-driven automation
Automatically use recipient responses to trigger actions and decisions within workflows, enabling dynamic, real-time process automation.

Low-code / no-code enablement
Build powerful communication workflows without bespoke development using Power Apps, Power Automate, Logic Apps, and Copilot Studio.

Seamless Power Platform integration
Embed messaging directly into existing Microsoft business applications and processes, extending their capabilities with minimal effort.

Scalable bulk and individual messaging
Send personalised messages to single recipients or deliver high-volume communications to large audiences from the same workflows.

Inbound engagement capture
Ingest end-user initiated replies and interactions directly into business processes for follow-up, escalation, or resolution.

Improved customer experience
Communicate through familiar channels without requiring users to change behaviour, increasing engagement and response rates.

Faster time-to-value
Eliminate the need for custom integrations or telecom development, allowing solutions to be deployed quickly and efficiently.

Future-ready communication foundation
Adopt a flexible messaging platform that supports evolving communication needs and can scale alongside your Power Platform solutions.

Dynamics 365 Messaging Plug-In

Boomerang's plug-in enables instant access to SMS messaging from any Dynamics 365 application. Where SMS solutions for Dynamics have traditionally been used to broadcast and notify, Boomerang's plug-in overcomes this limitation, automatically matching SMS activities and their associated responses. This enables Dynamics' users to create conversational engagements with stakeholders, as all outbound messages and responses are recorded in a contact's timeline. Crucially, this also creates an opportunity to drive real-time automation into a range of Dynamics' workflow processes, where a response is used as a trigger to initiate further steps in a workflow.

Features

Simple integration with Microsoft Dynamics 365
Designed specifically for use with Dynamics 365 via a dedicated plug-in

Intelligent two-way / conversational messaging
Enables replies to be tracked and mapped directly to outbound messages, supporting full conversations.

Low-code / no-code enablement
Allows business users to build communication workflows without bespoke development.

Workflow automation and orchestration
Integrates messaging directly into D365 business processes to automate tasks and decisions.

Delivery confirmation and inbound response triggers
Provides triggers for delivery status updates and SMS response submissions.

Inbound Communications
Allows retrieval of end use initiated inbound SMS messages to feed into Dynamics workflows

Delivery Receipts (DRs) Retrieval
Provides detailed delivery status updates with paging, filtering, and deduplication support.

Social Hours & Time-Zone Control
Restricts message delivery to defined business hours using recipient location, time zones, or UTC offsets.

UI Access for reporting and analytics
Access to the Boomerang interface for real-time tracking of transactional message data, delivery status information and analytical insights.

Benefits

Rapid Deployment and Reduced Complexity
Reduces implementation effort and accelerates time to value by enabling organisations to adopt SMS messaging quickly within existing Dynamics 365 environments.

Stronger Customer Engagement Through Conversations
Improves customer engagement and service effectiveness by allowing replies to be tracked, linked to outbound messages, and managed as complete conversations within Dynamics workflows.

Business-Led Configuration and Agility
Empowers business users to design, modify, and maintain communication workflows without bespoke development, reducing reliance on technical resources and speeding up change.

Operational Efficiency Through Automation
Increases efficiency by embedding messaging directly into Dynamics 365 business processes, enabling automated actions, decisions, and follow-ups driven by message events.

Reliable Event-Driven Processes
Enhances process reliability by triggering automated actions based on message delivery confirmations and inbound SMS responses from end users.

Improved Responsiveness to Customer Initiated Contact
Enables organisations to capture and process inbound, customer-initiated SMS messages directly within Dynamics queues and workflows for faster handling and resolution.

Transparency, Compliance, and Auditability
Provides clear visibility into message delivery outcomes through detailed delivery status information, supporting auditing, monitoring, and reporting requirements.

Customer-Friendly and Compliant Messaging
Protects customer experience and supports compliance by ensuring messages are delivered only during approved business hours based on recipient location or time-zone rules.

Actionable Insights and Performance Visibility
Supports better operational insight and decision-making by providing real-time access to transactional messaging data, delivery status information, and analytical reporting through the Boomerang user interface.

A full specification for Microsoft Messaging is available in Appendix D

4.5 Email-to-SMS and Email-to-Voice Messaging

Boomerang's Email-to-SMS and Email-to-Voice services allow organisations to send 1-Way or conversational SMS and voice messages directly from a local email client. Using 'Intelligent' messaging, 2-way conversations are managed automatically, with communication threads grouped by subject rather than time. This ensures that users can easily maintain and manage separate conversations in their email inbox. As all outbound messages and associated responses are recorded, corporate governance and regulatory compliance are maintained.

Features

Email-to-SMS and Email-to-Voice Conversion
Sends SMS or text-to-speech voice messages directly from an email client.

1-Way, 2-Way, and Conversational Messaging Support
Enables outbound-only messaging or full conversational threads with replies returned via email.

Secure Access Controls
Restricts service access by authorised email domains, individual email addresses, IP addresses, or mail servers.

SPF-Based Anti-Spoofing Protection
Prevents email spoofing by validating sender IP addresses against SPF records.

Fixed or Dynamic SMS Originator Options
Allows configuration of alpha originators for SMS, including fixed originator support.

Message Management Tools
Includes character limits, message disclaimers, and signature management to control outbound content.

Delivery Status Notifications
Provides email alerts for failed or undeliverable messages returned by network operators.

Social Hours Scheduling
Controls when messages are sent to ensure delivery only during approved time windows.

Advanced Reporting and Dashboard
Offers real-time dashboards and customizable transaction reports with graphical and tabular views.

Benefits

No New Software Required
Users can send SMS and voice messages directly from their existing email clients.

Faster and Simpler Communication
Enables rapid outreach to mobile users without complex integrations or APIs.

Improved Engagement Through Two-Way Messaging
Supports conversational messaging, allowing recipients to reply and continue interactions via email.

Enhanced Security and Compliance
Strong access controls, SPF validation, and secure data handling reduce the risk of unauthorised use.

Global Reach from a Single Platform
Communicate with recipients worldwide using SMS or voice without managing multiple providers.

Consistent Brand Presentation
Custom originators, signatures, and disclaimers ensure messages align with brand and compliance standards.

Reduced Messaging Errors
Character limits and validation prevent messages from being sent incorrectly or incompletely.

Greater Control Over Message Timing
Social Hours help avoid sending messages outside acceptable or regulatory-approved timeframes.

Operational Visibility and Accountability
Delivery status notifications and detailed reporting improve traceability and issue resolution.

Actionable Insights and Performance Tracking
Comprehensive reporting enables monitoring of usage, costs, delivery success, and recipient engagement.

A full specification for Email-2-SMS and Voice Messaging is available in Appendix E.

4.6 Inbound Communications

Inbound Campaign Management enables organisations to efficiently handle high-volume inbound communications triggered by campaigns or events. The service supports scalable routing, prioritisation, and real-time handling of inbound interactions across multiple channels, ensuring messages are received, processed, and responded to reliably. Campaigns can be connected to Logic workflows, allowing end-user-initiated engagements to automatically trigger defined business processes. Built on a resilient, cloud-based platform, it adapts to demand surges, provides visibility of campaign performance, and helps organisations maintain service levels while delivering timely and consistent responses to end users.

Features

Multi-Channel Inbound Support
Receives messages across SMS, Email, WhatsApp, and other supported channels.

Message Normalisation
Standardises inbound message data into a consistent model regardless of channel.

Configurable Handler Rules
Client-defined handlers control how inbound messages are matched and processed.

Matching Logic
Uses clear, predictable rules for channel, address, wildcard, and keyword matching.

Wildcard and Exact Address Matching
Supports exact, partial, and global wildcard matches for flexible routing.

Keyword-Based Message Recognition
Enables strict prefix keyword matching to distinguish commands or intents.

Initiate Logic Workflows
Routes matched messages to non-blocking, scalable processing workflows.

Automated Reply Capability
Sends configurable auto-responses on the same inbound channel.

Attachment Handling
Supports structured inbound attachments with metadata and base64 encoding.

Searchable Reporting and Analytics API
Provides filterable, paginated, and ordered access to inbound message data.

Benefits

Centralised Inbound Communication Management
Consolidates multiple communication channels into a single service.

Improved Operational Efficiency
Automates routing and processing, reducing manual handling of inbound messages.

Scalable and Non-Blocking Design
Handles high message volumes without delaying message receipt.

Flexible Routing for Complex Use Cases
Supports dedicated addresses, shared inboxes, and catch-all configurations.

Faster Customer and User Responses
Immediate auto-replies improve responsiveness and user experience.

Customisable Business Logic
Client-defined handlers and workflows adapt easily to changing requirements.

Reliable Audit and Compliance Records
Persistent message and handler-match storage support auditing and traceability.

Actionable Insights and Reporting
Searchable statistics enable monitoring, analysis, and optimisation of inbound traffic.

Seamless System Integration
Easily triggers workflows and forwards data to internal or external systems.

Reduced Risk of Message Loss
Wildcard and fallback handlers ensure all inbound messages are captured and processed.

A full specification for Inbound Communications is available in Appendix F.

4.7 Monitoring & Alerting

Inbound Monitoring and Alerting provides automated detection of service issues by continuously checking configured endpoints or conditions and evaluating their health. When a check completes or a status changes, the service generates structured alerts and passes monitoring data into Logic workflows for automated response. This enables rapid identification of failures, confirmation of recovery, and triggering of notifications or remedial actions, helping organisations respond proactively to incidents without manual intervention.

Features

Automated scheduled monitoring
Monitors run automatically on configurable schedules with defined frequencies, days, and time windows.

Multiple monitor types
Supports both Ping monitors (URLs and APIs) and Weather monitors for external condition tracking.

Configurable liveness and recovery checks
Each ping monitor includes a mandatory liveness check and an optional recovery check with independent criteria.

Advanced ping configuration options
Checks support custom URLs, ports, headers, timeouts, expected response codes, and response body matching.

Monitor lifecycle management
Monitors move through draft, active, and archived states, with execution limited to active monitors only.

Real-time status tracking
Maintains current health state, last check result, and next scheduled run time for each monitor.

Automated trigger dispatching
Monitoring events generate structured triggers containing status, metadata, and response details.

Workflow-based alerting and response
Alerts and responses are handled through Boomerang's configurable workflow engine within each customer account.

Secure configuration handling
Sensitive values are encrypted at rest, decrypted only at runtime, and protected through sanitisation and secure logging.

Transactional data management
Monitor creation, updates, and deletion are handled transactionally to ensure consistency and prevent orphaned data.

Benefits

Proactive issue detection
Continuous monitoring identifies failures early, reducing downtime and customer impact.

Consistent and automated incident response
Predefined workflows ensure alerts, escalations, and communications follow standardised processes.

Reduced operational overhead
Automation eliminates manual checks and repetitive alerting tasks for operations teams.

Faster recovery and resolution times
Recovery checks and automated workflows confirm service restoration and notify stakeholders quickly.

Improved visibility into service health
Teams gain real-time and historical insight into availability, performance, and incident trends.

Flexible monitoring aligned to business needs
Scheduling windows, exclusions, and custom variables allow monitoring to match operational calendars and priorities.

Context-rich alerts
Structured trigger data provides detailed information, enabling faster diagnosis and informed decision-making.

Policy-driven communications
Alerts can be routed and escalated based on severity, duration, or context, aligning with organisational policies.

Strong security and data protection
Encrypted configuration values and secure handling reduce the risk of data exposure or misuse.

Scalable and resilient operations
Asynchronous trigger processing and transactional data handling support reliable monitoring as environments grow.

A full specification for Monitoring & Alerting is available in Appendix G.

4.8 Logic Solutions

Solutions are pre-configured, outcome-focused communication and automation workflows delivered as cloud services. Each Solution fulfils a specific business process (such as appointment rescheduling, incident communications, mustering, or 2FA) and is purchased individually. Solutions use Logic workflows to orchestrate multi-step processes, combining multi-channel messaging, response capture, conditional logic, escalation, and reporting. They can be delivered via secure API integrations with third-party systems or executed directly through a user interface, providing operational visibility, auditability, and configurable governance without the need for bespoke development.

Features

Pre-configured, ready-to-use workflows
Solutions are delivered as pre-built workflows tailored to specific business processes.

Configurable without bespoke development
Workflow logic, content, channels, timing, and rules can be adjusted to customer needs without custom coding.

Multi-channel communication support
Supports SMS, Email, Voice, WhatsApp, RCS, and web forms within a single workflow.

Workflow orchestration and automation
End-to-end processes are automated using triggers, timers, conditional logic, and parallel actions.

Two-way response capture and handling
Structured responses via messages or forms are captured and processed automatically.

API-based system integration
Secure APIs enable integration with third-party systems such as CRMs, booking platforms, and service desks.

User interface-driven execution
Workflows can be launched and managed directly through the platform UI without external system integration.

Escalation and exception management
Built-in escalation paths handle non-responses, failures, and critical events automatically.

Real-time reporting and dashboards
Provides visibility into delivery, response rates, workflow status, and SLA performance.

Governance, auditability, and role-based access
Centralised templates, version control, audit logs, and permissions ensure controlled and compliant usage.

Benefits

Faster deployment and time to value
Pre-configured Solutions significantly reduce implementation effort and rollout times.

Reduced development and IT overhead
Configuration replaces bespoke development, lowering cost and reliance on specialist resources.

Improved communication reach and reliability
Multi-channel delivery with fallback and escalation increases successful engagement.

Consistent and repeatable business processes
Standardised workflows ensure reliable execution across teams and use cases.

Enhanced operational efficiency through automation
Manual tasks are reduced, freeing staff to focus on higher-value activities.

Better decision-making through captured responses
Structured response data enables automated decisions, reporting, and follow-up actions.

Seamless integration with existing systems
API-driven workflows enable end-to-end automation without disrupting current platforms.

Greater visibility and control over operations
Real-time dashboards support proactive monitoring, SLA management, and issue resolution.

Improved compliance and audit readiness
Full audit trails, governed templates, and access controls support regulatory requirements.

Scalable and flexible solution model
Individually purchased Solutions allow organisations to adopt only what they need and scale over time.

A full specification for Logic Solutions is available in Appendix H

4.9 AI Services

Boomerang AI Services provide a secure, governed platform enabling customers to create and use AI-driven solutions through APIs, email integrations, and a user interface. The service supports document processing, summarisation, comparison, extraction, content creation, automation, and aggregation across multiple data sources. It includes reporting, dashboards, usage visibility, and logging of all AI-driven actions, with shared and exclusive service models offering different levels of control, data governance, and access. These capabilities help organisations automate tasks, generate insights, and make informed decisions while meeting regulatory and operational requirements.

Features

- **AI- and LLM-enabled platform** accessible via secure web UI, email, and APIs
- **Document and data processing capabilities**, including summarisation, extraction, classification, and content generation

- **Natural-language interaction** for querying, transforming, and generating information
- **Workflow automation and decision-support tools** configurable to organisational needs
- **Multi-document and dataset aggregation and analysis** for cross-source insights
- **Structured data extraction and output generation** from unstructured content
- **Document comparison and change detection** to identify inconsistencies or updates
- **Content governance functions**, including redaction, anonymisation, and masking
- **Role-based access controls, approvals, and audit logging** for AI activity
- **Reporting dashboards** covering usage, performance, compliance, and system health

Benefits

- **Improved operational efficiency** by automating repetitive and time-consuming tasks
- **Enhanced decision-making** through faster access to insights, trends, and risk indicators
- **Reduced manual effort and errors** in document handling and data processing
- **Consistent and accurate outputs** across users, workflows, and departments
- **Seamless integration with existing systems** via APIs and email-based workflows
- **Greater transparency and accountability** through logging, reporting, and audit trails
- **Stronger data protection and compliance** with configurable governance controls
- **Flexible deployment options** that balance cost, capability, and data isolation needs
- **Scalable AI usage** that adapts to changing workloads and organisational priorities
- **Public-sector-ready AI adoption** aligned with regulatory, security, and G-Cloud principles

A full specification for AI Services is available in Appendix I.

---

5 Approach to Information Assurance

5.1 Overview

The organisation operates a comprehensive Information Security Management System (ISMS) that governs the management and protection of customer information and service data. The ISMS is aligned to recognised international standards and UK government guidance and is subject to ongoing review and continuous improvement.

Accreditations and Standards

The organisation holds the following current certifications and independent assurances:

- ISO/IEC 27001:2022 – Information Security Management
- Cyber Essentials and Cyber Essentials Plus
- Financial Services Qualification System (FSQS) – Stage 3 Approved Supplier

In addition, the organisation aligns its security and operational practices with the following recognised standards and principles:

- ISO/IEC 22301 – Business Continuity Management
- ISO 9001 – Quality Management
- ISO/IEC 27701 – Privacy Information Management
- NCSC Cloud Security Principles

5.2 Information Security Management System (ISMS)

The ISMS applies across the organisation, its staff, the cloud services offered, and relevant supply chain activities that process or may access customer data. It includes a documented statement of applicability, defined security objectives, and a risk-based control framework aligned to ISO/IEC 27002:2022.

The ISMS includes:

- Risk assessment and ongoing risk management processes covering customer information and related information assets, based on confidentiality, integrity, and availability (CIA).
- Selection and implementation of proportionate technical and organisational controls aligned with ISO/IEC 27002:2022.
- Defined governance arrangements, including management oversight, performance monitoring, internal audits, independent audits, corrective actions, and continual improvement.
- Regular information security awareness training for all staff, supported by an HR security lifecycle covering recruitment, onboarding, role changes, and leavers.

Security Controls

Security controls are implemented and maintained in line with ISO/IEC 27002:2022 and include organisational, people, physical, and technological controls covering, but not limited to:

- Governance, risk management, and information security policies
- Human resources and personnel security

- Asset management and information classification
- Identity and access management
- Cryptography and key management
- Secure configuration, logging, and monitoring
- Secure development and change management
- Physical and environmental security
- Supplier and third-party security
- Incident management and event reporting
- Business continuity and resilience
- Compliance with legal, regulatory, and contractual requirements

Incident Management and Business Continuity

Information security incidents are managed in accordance with documented procedures, including identification, triage, containment, investigation, and recovery. Personal data breaches are assessed promptly and, where required, reported to the Information Commissioner's Office (ICO) and affected individuals within statutory timescales, in line with UK GDPR and the Data Protection Act 2018.

Business continuity and disaster recovery arrangements are aligned to ISO/IEC 22301 and are designed to support the availability and resilience of the service.

Data Protection and Privacy

The organisation processes personal data in accordance with UK GDPR and the Data Protection Act 2018. Privacy and data protection controls are embedded through:

- Privacy by design and default
- Documented processes for handling Subject Access Requests (SARs)
- Data breach notification and escalation procedures
- Data protection impact assessments (DPIAs) for relevant processing activities

Privacy management controls are aligned to ISO/IEC 27701.

Supplier and Shared Responsibility Model

The organisation operates a shared responsibility model for information security. The organisation is responsible for the security of the service, infrastructure, and operational controls under its management. Customers are responsible for the secure configuration and use of the service in accordance with provided guidance.

All suppliers with access to customer data are subject to due diligence, contractual security obligations, and ongoing assurance proportionate to the risk they present.

Policy Management and Assurance

Information security policies and supporting ISMS documentation are reviewed at least annually or following significant change. A public summary of the Information Security Policy is available on the organisation's website, with additional assurance documentation available to customers upon request under appropriate confidentiality arrangements. Boomerang's Information Security Policy is reviewed at least annually and is available on the company website.

6 Business Continuity Management and Disaster Recovery Provision

Boomerang is responsible for ensuring the resilience and continuity of the Service through a comprehensive Business Continuity and Disaster Recovery (BCDR) framework. This framework is designed to minimise disruption, protect service availability, and ensure rapid recovery from incidents affecting people, processes, technology, or suppliers.

Our approach is aligned with ISO 22301 (Business Continuity Management), ISO 27001, Cyber Essentials Plus, and ITIL best practice, and is reviewed and approved annually by senior management.

6.1 Business Continuity Management

Boomerang maintains formal Business Continuity Plans (BCPs) covering all critical business functions supporting the Service. The objectives of the BCP are to:

- Maintain continuity of critical service operations
- Minimise the impact of disruptive incidents
- Enable a controlled and timely return to business-as-usual
- Safeguard staff, customers, assets, and information

Business continuity planning is underpinned by regular Business Impact Analysis (BIA) and risk assessments to identify critical processes, dependencies, acceptable service loss, and recovery priorities.

BCP arrangements include:

- Defined escalation and incident management procedures
- Clear roles and responsibilities
- Communication plans for customers and stakeholders
- Staff awareness and training
- Consideration of supplier and third-party dependencies
- Annual review and approval by the CEO and Operations Director

Plans are maintained to reflect changes in business operations, technology, or risk profile.

6.2 Service Resilience and Architecture

The Service is architected to **eliminate single points of failure** and provide high availability across infrastructure, platform, and application layers.

Infrastructure and Hosting

- The Service operates across multiple UK-based data centres with real-time data replication between geographically separated locations.
- Automatic multi-site failover is in place, enabling immediate service continuity in the event of infrastructure or network failure.
- All data centres meet recognised industry security and resilience standards.

Cloud Platform

- The Service is delivered on a clustered, cloud-based platform using VMware and Kubernetes.
- The platform supports automatic scaling, ensuring resilience during demand spikes.
- Designed to achieve 99.99% service availability.

Network Resilience

- Redundant, carrier-diverse network connections are in place at all internet-facing edges.
- Multiple high-capacity connections across diverse UK network providers ensure resilience and performance.
- DDoS protection, intrusion detection, and continuous network monitoring are implemented.

Application Resilience

- Services are deployed across multiple instances with load balancing.
- Modular architecture allows individual components to scale independently.
- Multiple messaging suppliers and queues are used to ensure continuity across communication channels.
- Real-time rollback is supported via snapshot-based recovery.

6.3 Backup and Data Recovery

Rigorous back up processes have been implemented to safeguard data.

- Full daily backups are taken and stored off-site.
- Hourly checkpoints are maintained on a rolling 30-day basis.
- Backups are retained for 365 days.
- All backups are verified and regularly tested to ensure successful restoration.
- Data is replicated to secondary storage nodes to maintain availability and integrity.

6.4 Monitoring and Capacity Management

Comprehensive, real-time monitoring is implemented across the Service using industry-standard tooling. This includes monitoring of:

- Service availability and performance
- Infrastructure health (CPU, memory, storage, databases)
- Network traffic and anomalies
- Supplier service performance
- Transactional throughput and messaging success rates

Threshold-based alerts trigger proactive incident response. Capacity and performance metrics are reviewed regularly to ensure the Service continues to meet customer demand and service levels. The platform can be scaled without disruption to live services.

6.5 Change and Maintenance Resilience

Boomerang applies a structured change management process to control modifications to systems, configurations, software and infrastructure.

- All changes are managed through a formal change management process.
- Changes are risk-assessed, approved, and tested prior to deployment.
- Testing is conducted in environments consistent with production.
- Maintenance and updates are performed out of hours where possible, with rollback procedures in place.
- Customers are notified in advance of planned changes in line with support arrangements.

6.6 Disaster Recovery

Boomerang maintains a detailed Disaster Recovery Plan to restore services quickly following a major incident.

- Recovery Time Objective (RTO): 30 minutes
- Recovery Point Objective (RPO): no more than one hour
- Real-time automated failover across multiple data centres.
- Backup restoration procedures tested routinely.
- Incident communication plans ensuring rapid and accurate notifications to affected stakeholders.
- Regular DR exercises, including technical failover and tabletop scenarios, with results logged and improvement actions tracked.

6.7 Testing and Continuous Improvement

Boomerang conducts a structured programme of testing and continuous improvement to ensure that Business Continuity and Disaster Recovery arrangements remain effective, up to date, and capable of meeting service commitments. This includes:

- Business Continuity and Disaster Recovery plans are tested at least quarterly, with different elements tested to ensure full annual coverage.
- Testing includes tabletop exercises and technical failover scenarios.
- Test outcomes are formally recorded, reviewed by senior management, and tracked to closure.
- Lessons learned are used to drive continual improvement of resilience controls.

6.8 Buyer Assurance

This resilience and business continuity approach ensures that public sector buyers receive a highly available, secure, and recoverable service, with clearly defined recovery objectives, tested controls, and governance aligned to recognised international standards.

---

7 Securing the services

The services are designed and operated in accordance with recognised information security standards and best practice, including ISO/IEC 27001, UK GDPR, and the NCSC Cloud Security Principles. Security controls are implemented using a defence-in-depth approach to protect data, systems, and users throughout the service lifecycle.

7.1 Network security

Network security controls are implemented to protect service boundaries and internal network segments in line with NCSC Cloud Security Principle 1 (Network Security).

Firewalls and other boundary protection devices are deployed at the network perimeter and between key internal network zones. These devices enforce traffic flow policies using access control lists (ACLs) and rulesets that restrict communications to authorised services, ports, and protocols only.

The network is logically segmented to separate web, application, database, and audit logging tiers, reducing the impact of any potential compromise and limiting lateral movement.

Automated monitoring systems are used to monitor network traffic, system availability, and security events. These systems detect unusual or unauthorised activity, including abnormal traffic patterns, port scanning, and intrusion attempts. Alerts are generated where predefined thresholds are exceeded and are handled in accordance with the incident management process.

7.2 Cloud and platform security

The service has been designed and implemented in accordance with the NCSC Cloud Security Principles.

Administrative access to the platform is protected using encrypted VPN connectivity and is restricted by firewall rules and access control lists. Access is granted only to authorised personnel and is subject to formal change control, approval, and regular review.

External access to the platform follows a layered security approach:

- Inbound connections are filtered by external firewall controls
- Approved traffic is further validated by internal firewall systems
- User access is granted only following successful authentication and authorisation

Network-level controls are complemented by identity-based access controls to ensure that access decisions are not based solely on IP address.

The platform architecture is tiered (web, application, database, and logging), allowing access to be restricted to individual components as required. Access permissions, including elevated (Sudo) privileges, are granted on the basis of least privilege and are reviewed regularly.

Independent external security scans and penetration testing are conducted to validate the effectiveness of platform security controls.

7.3 Application security

The service uses a modular application architecture, with components logically separated and secured independently. Communication between components is protected using encrypted channels.

All service access points, including web interfaces and API endpoints, are protected using **TLS (HTTPS)** with industry-standard cipher suites to protect data in transit.

Security is embedded throughout the software development lifecycle in line with NCSC Cloud Security Principle 7 (Secure Development). A Secure Development Policy ensures that:

- Access to development environments is restricted and granted on a need-to-know basis
- Development and test environments are appropriately secured and segregated from production
- Security requirements are considered during design and planning
- Code is developed in line with recognised best practices (such as OWASP guidance) and stored in secure version control repositories
- Security testing forms part of the testing and release process

7.4 Malware prevention

Malware protection controls are implemented across the service infrastructure.

Automated malware scanning is deployed on servers and supporting systems, using regularly updated signatures and detection mechanisms. Monitoring tools are used to identify potentially malicious activity, including indicators of compromise or unauthorised changes.

Operational staff are trained to recognise and respond to suspected malware incidents. Any detected malware is isolated and quarantined, and alerts are raised internally for investigation and remediation in line with the incident management process.

7.5 Security and vulnerability testing

Security testing is carried out regularly to ensure that the service remains protected against known vulnerabilities and emerging threats, in line with NCSC Cloud Security Principle 4 (Monitoring and Auditing).

This includes:

- Independent penetration testing of the service infrastructure at least annually
- Regular vulnerability scanning of all service components
- Web application security testing aligned to recognised standards such as the OWASP Top 10
- Continuous monitoring for common vulnerabilities and misconfigurations

Identified vulnerabilities are risk-assessed, prioritised based on severity, and remediated within defined timescales.

7.6 Securing data

Cryptographic controls

Cryptographic controls are used to protect data at rest and in transit, in line with NCSC Cloud Security Principle 5 (Data Protection).

Data in transit

All access to the service via web interfaces or APIs is protected using TLS encryption. This applies to desktop and mobile access.

Data at rest and backups

Backup data is encrypted using AES-256 encryption. Encryption keys are securely generated, stored, and managed using controlled key management processes, with access restricted to authorised personnel only.

When storage media reaches the end of its useful life, data is securely destroyed in accordance with NIST SP 800-88 (Guidelines for Media Sanitization) to prevent unauthorised data recovery.

Databases

Sensitive data stored within databases is protected using encryption mechanisms provided by the database platform. Encryption is applied to protect data throughout its lifecycle.

7.7 Access controls

Access to systems and data is governed by formal access control policies aligned to NCSC Cloud Security Principle 6 (Identity and Authentication).

Internal access controls

- Access to systems processing customer data is granted on the basis of least privilege
- All access is formally authorised and subject to regular review
- Each user is assigned a unique user ID
- Security-relevant actions are logged with date and time stamps
- Asset owners are responsible for reviewing access rights and ensuring they remain appropriate

Audit logs are protected from unauthorised modification and are reviewed to support security monitoring and investigation.

Customer access controls

Customer access to the service is protected by authentication controls, password management, and optional multi-factor authentication. Role-based access controls allow customers to define permissions aligned to job roles and responsibilities.

Customers can control access to personal and transactional data on a need-to-know basis, and data can be anonymised where required.

Customers retain control of the data they submit to the service and can modify or delete it at any time. Customer data is deleted following the end of a trial or contract period in

accordance with agreed retention policies. Access to customer data by service staff is restricted and occurs only at the customer's request or where required to investigate service-related issues.

7.8 Staff recruitment and training

Personnel security controls are implemented in line with NCSC Cloud Security Principle 8 (Personnel Security).

Appropriate pre-employment screening and checks are carried out for employees and contractors. All personnel are required to comply with the organisation's information security policies as part of their contractual obligations.

Information security training is provided at regular intervals and is recorded as part of each individual's development plan. Updates on emerging threats, security issues, and regulatory requirements are communicated to staff as needed.

Compliance with security policies and procedures is verified through regular internal and external audits.

7.9 Data retention and legislative compliance

Data flows involving personal data have been mapped across the organisation. Data retention policies are implemented to ensure that data is retained only for as long as necessary and in accordance with the purpose for which it was collected.

The service is operated in compliance with applicable data protection legislation, including UK GDPR and the Data Protection Act 2018.

Procedures are in place to identify, manage, and report personal data breaches in accordance with regulatory requirements and contractual obligations.

---

8 Customer On-Boarding & Off-Boarding

8.1 On-Boarding

Our on-boarding process is designed to ensure customers can begin using the service quickly, securely, and with minimal disruption.

Once an order is confirmed, we will work with the customer to agree an implementation plan covering timescales, responsibilities, and any service-specific configuration requirements. A named point of contact will be provided for the duration of the on-boarding process.

On-boarding activities may include:

- Account creation and user access setup
- Configuration of the service in line with customer requirements
- Integration with customer systems, where applicable
- Security and access controls aligned to customer policies
- Data migration or initial data upload (if required and agreed)

- User guidance and onboarding documentation
- Training

The service is delivered using standardised processes to minimise risk and ensure consistency. Any customer dependencies or prerequisites will be clearly communicated in advance. Where applicable, testing or validation will be completed before the service is made live.

There is no additional charge for standard on-boarding unless otherwise stated in the pricing document.

8.2 Off-Boarding

Our off-boarding process ensures that customers can exit the service in a controlled, secure, and transparent manner at the end of the contract or upon termination.

Upon receiving notice to off-board, we will agree an exit plan with the customer, including timelines and any specific requirements. Off-boarding activities may include:

- Secure extraction and return of customer data in a commonly used format
- Confirmation of data ownership and transfer arrangements
- Deactivation of user accounts and access credentials
- Removal of customer-specific configurations
- Secure deletion of customer data from our systems in line with our data retention and destruction policies
- Confirmation of service termination

Data will be handled in accordance with applicable data protection legislation, including the UK GDPR. Data deletion will be completed within agreed timescales following contract termination, unless otherwise required by law.

Where requested, we will provide reasonable assistance to support transition to an alternative supplier. Any additional off-boarding support beyond standard activities may be subject to additional charges, which will be agreed in advance.

---

9 Service Management

9.1 Background and Overview

Boomerang provides a cloud-hosted Software as a Service (SaaS) solution designed for use by UK public sector organisations. The services are accessed via a secure web-based user interface and/or Application Programming Interfaces (APIs). No local software installation or downloads are required*.

The service has been designed to operate in accordance with relevant UK legislation and government policy, including environmental and sustainability objectives. Ongoing service management activities are delivered in line with G-Cloud 15 requirements.

*Excludes Plug-In for Dynamics 365

9.2 Operational Services

Account administration

Boomerang will provide a user interface or managed service for the customer which will include the ability to achieve the following:

- Provision and management of account configuration and settings
- Provision of other service users and management of access
- Addition of services, products, or features
- Amendment of existing service, product, or feature selections
- Access to transactional messaging data reports

Reporting

Customers have access to transactional and analytical reporting data relating to their use of the service via the user interface. Reporting access is controlled by user permissions. Reports can be viewed online and exported in standard formats.

9.3 Training services

Training is provided as part of the onboarding process and is delivered remotely (telephone or online) unless otherwise agreed. Training sessions are arranged by the customer's Account Manager in collaboration with the customer.

As standard, onboarding training covers:

- Account configuration and administration
- Service overview and provisioning
- Use of the user interface
- Reporting
- Billing
- Support processes

Additional or refresher training can be provided on request and may be chargeable. Training can be delivered in an accessible format where required.

9.4 Service Constraints and Maintenance

Maintenance activities are categorised as follows:

Planned Maintenance

Planned maintenance includes scheduled activities required to maintain service security, stability, and performance. Where possible, planned maintenance is scheduled to minimise disruption.

- Customers receive a minimum of **5 working days' notice**
- Notifications are issued to designated contacts before and after maintenance
- Planned maintenance is excluded from availability calculations

Unplanned Maintenance

Unplanned maintenance may be required to prevent or mitigate service degradation or potential service disruption. Where possible, customers will be informed during the activity.

Emergency Maintenance

Emergency maintenance is carried out to address critical issues affecting service availability, performance, or security. Due to the urgent nature of such work, advance notice may not be possible.

9.5 Operational service support

Operational support includes incident management and service requests.

Support requests are logged and tracked using Boomerang's technical support case management system and may be raised by authorised customer contacts or by Boomerang on the customer's behalf.

Incident Priority Levels

Support incidents are prioritised as follows:

- **Priority 1 (High):** Complete loss of service or a critical issue with significant business impact
- **Priority 2 (Medium):** Partial loss of service or significant degradation of functionality
- **Priority 3 (Low):** Non-critical issues, general queries, or service requests

Service requests may include "how-to" queries, billing enquiries, and service change requests.

9.6 Support packages

Two support packages are available: **Standard Support** and **Premium Support**. Standard Support is included as part of the base service. Premium Support is optional and chargeable.

Premium Support may be provided on an annual term. Alternative terms may be agreed with public sector customers

Support element	Standard Support	Premium Support*
Support availability		
Support times	9am-6pm, Mon-Fri (UK)	24/7/365
Support channel	Email	Email, Telephone
System availability		
Target availability	No commitments	99.50%
Issue response times		
Severity level 1	No commitments	1 hour
Severity level 2	No commitments	1 hour
Severity level 3	No commitments	1 hour

Service Restoration Target		
Severity level 1	Best endeavours	3 hours
Severity level 2	Best endeavours	12 hours
Severity level 3	Best endeavours	2 working days
Scheduled Maintenance		
Notice period	Minimum 5 days	Minimum 5 days
Actions per month	No commitments	Maximum of 2
Terms		
Minimum term	N/A	12 months
Subscription Payment Terms	N/A	Annual in advance

*Premium Support is chargeable as per G-Cloud 15 Price List.

9.7 SLA penalties and service credits

Customers with Premium Support are eligible for Service Credits where Boomerang fails to meet the monthly System Availability target of **99.50%**.

System Availability is measured on a calendar-month basis and excludes periods of planned maintenance notified in advance.

Where the availability target is not met, the customer may claim a Service Credit equal to 10% of the monthly subscription fee for the affected service (calculated as one twelfth of the annual subscription).

Service Credits:

- Apply only to the service subscription fee
- Do not apply to usage-based charges or third-party costs
- Must be claimed within **30 days** of the end of the affected month

Service Credits are not available where the customer is in material breach of the agreement, including non-payment at the time the outage occurred.

9.8 Account Management Service

Each customer is assigned an Account Manager who acts as the primary point of contact for service management and ongoing engagement.

Account Management Responsibilities

The Account Manager is responsible for:

- Coordinating service onboarding
- Acting as a point of escalation for service-related issues
- Providing regular service reviews and performance updates

The customer is responsible for:

- Nominating appropriate operational, technical, and commercial contacts

- Participating in agreed service review meetings

Service Reviews and Reporting

The standard account management model includes:

- A post-implementation check-in
- Quarterly service review meetings conducted remotely unless otherwise agreed

The Account Manager will provide:

- Meeting notes and agreed actions
- Periodic service performance summaries

There are no contractual SLAs associated with account management activities.

Ordering and Invoicing

Customers may order additional services or features via the user interface or by issuing a purchase order. Invoices are issued electronically in PDF format, provided to designated billing contacts, and can also be accessed from Boomerang the user interface.

The standard billing model is as follows:

- Service subscriptions are charged annually in advance
- Usage-based charges are billed monthly in arrears or deducted from pre-paid credits
- Invoices include a breakdown of usage and associated costs

Alternative billing arrangements may be agreed for public sector customers and documented in the customer agreement.

Billing queries should be submitted in writing within 20 days of the invoice date. Unresolved queries may be escalated in accordance with Boomerang's billing procedures.

There are no contractual SLAs associated with ordering and invoicing activities.

---

10 Customer requirements & Technical Pre-requisites

10.1 Customer requirements

Customer requirements are defined in context within the relevant sections 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.

10.2 Technical pre-requisites

To use the service effectively, customers must ensure that the following technical pre-requisites are met:

User Devices and Access

- A modern web browser (latest or previous major release of Google Chrome, Microsoft Edge, Mozilla Firefox, or Apple Safari).
- JavaScript and cookies enabled within the browser.
- A stable internet connection with sufficient bandwidth to support normal service usage.

Network and Security

- Ability to access the service over HTTPS (TCP port 443).
- Customer networks must allow outbound connections to the service's URLs and APIs.
- Any customer-managed firewalls, proxies, or content filters must be configured to permit service traffic.
- For API access (where applicable), customers must support RESTful APIs over HTTPS.

Authentication and Identity (where applicable)

- Customer-managed user accounts, or integration with supported identity providers (e.g. SAML 2.0, OAuth 2.0, or Microsoft Entra ID / Azure AD).
- Customers are responsible for managing user credentials, roles, and access permissions unless otherwise stated.

Customer Responsibilities

- Provisioning and maintenance of end-user devices.
- Management of local network infrastructure.
- Compliance with internal security policies and relevant data protection obligations.
- Timely application of updates to any customer-managed systems that integrate with the service.

10.3 Service Constraints

The following constraints apply to the services:

Scope of Services

- The service is provided as described in the Service Definition. Functionality outside this scope is not included unless agreed via a separate contract.
- Custom development or bespoke configuration is not included unless explicitly stated.

Availability and Maintenance

- The service is designed to be available 24x7, excluding planned maintenance.
- Planned maintenance will be communicated in advance wherever possible and is typically conducted outside UK business hours.
- Emergency maintenance may be required to maintain service security or stability.

Performance and Usage

- Performance may be affected by customer network connectivity, device capability, or third-party dependencies.

- Fair usage policies may apply to prevent excessive or abusive consumption of system resources.
- Any published service limits (e.g. storage, user numbers, API calls) are defined in the service documentation.

Dependencies and Third-Party Services

- The service may rely on third-party components or cloud infrastructure providers.
- The supplier is not responsible for outages or issues caused by failures in customer systems or third-party services outside the supplier's control.

Data and Integration Constraints

- Data import/export is supported only in the formats documented for the service.
- Integrations are limited to supported APIs and interfaces.
- Customers are responsible for the accuracy and legality of data entered into the service.

Security and Compliance

- Customers must not attempt to circumvent service security controls.
- The service must be used in accordance with applicable laws and regulations.
- Any additional compliance requirements beyond those stated in the Service Definition may require separate agreement.

Appendix A - Functional specification for Boomerang CPaaS Messaging & Workflow Platform

1 Overview of CPaaS Messaging & Workflow Platform

The Boomerang CPaaS Messaging & Workflow Platform is a secure, cloud-based platform designed to orchestrate complex, event-driven communications and operational workflows across multiple channels and systems. At its core is the Logic Workflow Engine, a configurable orchestration layer that enables low-code/no-code workflow configuration for organisations to design, execute, and manage multi-step workflows with conditional logic, and automated decision points. Workflows can respond to real-time triggers, monitoring alerts from an integrated monitoring tool, user interactions, inbound messages, or system events.

The platform provides flexible API Connections that enable seamless integration with internal systems, third-party applications, and external data sources. These integrations allow workflows to exchange data, trigger actions, and synchronise state across systems.

The platform also includes access to a Broadcast Messaging Interface and function rich Messaging APIs for high-throughput, bi-directional messaging campaigns, Email-to-SMS and Voice capabilities, as well as Inbound Communication tools for receiving and processing end user initiated engagements which can seamlessly integrate with Logic workflows.

1.1 Platform Capabilities

Logic Workflow Engine - A configurable workflow orchestration engine that enables the design and execution of event-driven, conditional, and multi-step communication logic. It supports automation across messaging, APIs, and integrations, enabling complex customer journeys and business processes.

API Connections - A flexible integration layer that enables seamless connectivity between the platform and external or internal systems.

Assets – A repository for the operational resources an organisation needs to track. An Asset represents any customer-defined entity such as a project, building, vehicle, location group, team base, or similar resource. Assets enable targeted messaging, simplified contact management, and more efficient, context-aware communication workflows.

Monitoring - Comprehensive observability tools that provide real-time monitoring of endpoints, APIs, and a range of additional system resources, with connection to configurable alerting and escalation paths to proactively identify and resolve issues.

Events - Events and Incident Management capability that allows authorised users to create, manage and communicate operational events, incidents and alerts through a secure web-based interface.

Dashboards - Operational dashboards providing real-time visibility into messaging activity, workflows, system health, and key performance metrics. The dashboards enable users to

quickly monitor performance, manage campaigns, and access platform capabilities from a single interface.

Reporting - Built-in reporting capabilities for analysing messaging performance, workflow and campaign outcomes, and system usage, combined with ticketing features to support issue tracking, operational support, and audit requirements.

Settings Management - Centralised configuration and governance controls for managing users, roles, channels, integrations, security policies, and environment-specific settings across the platform.

Broadcast Messaging Interface - A high-throughput interface for creating, scheduling, and managing outbound broadcast messaging campaigns across supported channels.
Reference: Specification for Broadcast

Messaging API - A developer-friendly, API for access to extensive messaging capabilities, enabling the sending, receiving, and tracking of messages across supported channels.
Reference: Specification for Messaging API

Email-to-SMS and Voice - Functionality that converts inbound or outbound email messages into SMS or voice communications, enabling seamless cross-channel delivery and response handling. Ideal for bridging legacy email workflows with mobile and voice channels.
Reference: Specification for Email-2-SMS

Inbound Communications - Tools and services for managing inbound messaging use cases, including keyword campaigns, automated responses, and routing logic. Enables real-time engagement and data capture from inbound customer interactions.
Reference: Specification for Inbound Communications

Solutions - Pre-configured, use-case-driven solution templates that bundle messaging, workflows, and integrations to accelerate time-to-value for common business scenarios and industry-specific requirements. Solutions are not included by default and must be purchased separately as per the G-Cloud 15 CPaaS Messaging & Workflow Platform Price List.
Reference: Specification for Logic Solutions

---

2 Logic Workflow Engine

2.1 Overview

The Logic Workflow Engine is a configurable, omni-channel orchestration platform designed to manage event-driven, time-driven, and conversational messaging workflows across global communication channels. It supports simple broadcasts through to complex, multi-stage, bi-directional workflows, integrating with third-party systems, contact data, assets, tickets, calendars, and AI services.

This specification defines:

- Supported communication channels
- Messaging modes

- Workflow architecture and capabilities
- Core workflow components
- Broadcast and reply handling
- Time-based orchestration
- Actions, conditions, and integrations
- Security, governance, and extensibility

2.2 Communication Channels

boomLogic supports international messaging across the following channels:

Channel	Description
SMS	Global SMS delivery
Voice (TTS)	Text-to-speech voice messages
Voice Calls	Live call routing to defined numbers
Email	Non-geographic email messaging
WhatsApp	Rich messaging with branding and media
RCS	Rich Content Messaging with interactive elements

All channels support **1-way and 2-way communication**, subject to channel constraints.

2.3 Messaging Solutions

The following messaging solutions are supported:

One-Way Messaging

- Outbound-only notifications
- No reply handling
- Used for alerts, reminders, and broadcasts

Two-Way Messaging

- Recipients can reply
- Replies are captured and processed by workflows
- Supported across all channels

Intelligent Two-Way Messaging

Replies are matched to:

- Individual recipients
- Individual broadcast instances
- Workflow threads

Conversational Messaging

- Subject-based conversation threads
- Parallel or single-threaded conversations
- Conversations persist across channels
- Context-aware reply processing

Inbound Messaging

- Workflow activation via inbound:
    - SMS
    - Email
    - WhatsApp
    - RCS
    - API
    - UI submissions
- End users or systems can initiate workflows
- Store and group end user data

2.4 Workflow Engine Overview

The workflow engine fully configurable, allowing any type of communication workflow to be configured to meet a wide range of bespoke requirements. Workflows within the same project can actively interact, sending and receiving to and from each other, enabling fluid and dynamic workflow configurations.

- Fully configurable, no-code / low-code workflow builder
- Drag-and-drop workflow designer
- Multi-workflow orchestration within a project
- Workflows can trigger, consume, or interact with other workflows

Key Capabilities

The workflow engine supports:

- Multi-step workflows
- Conditional logic and branching
- Dynamic data-driven personalization
- Multi-channel orchestration
- External system integration
- Runtime simulation and testing

2.5 Workflow Architecture

A workflow consists of the following logical layers:

Activation → Data Extraction → Conditions → Actions → Milestones → Completion

Workflows may execute sequentially or in parallel and may persist over long durations.

2.6 Workflow Activation

Activation Channels

Workflows can be activated via:

- HTTPS / API
- Email
- SMS
- User Interface (manual or form-based)

- Integrated Monitoring Tools
    - Ping Monitor
    - Weather alerts
- Boomerang Third-party integrations

Activation Functions

Data extraction

- Extract recipient identifiers (SMS, email, voice)
- Extract structured and unstructured data
- Create workflow variables
- Tokenise data for message personalization
- Categorise recipients and variables dynamically
- Store and categorise data from inbound requests

Activation Criteria

Workflows may start:

- Immediately (on receipt of activation request)
- At a scheduled time
- After a delay
- Based on variable date/time values
- Relative to another event or date
- Localised to recipient time zones

Conditional Activation

Activation may depend on:

- Content of inbound requests
- Keywords or values
- Counts of inbound requests
- Absence of inbound requests within a time window
- Sender identity or channel
- Recipient attributes or group membership
- Pre-configured monitoring conditions

Validation

Requests can be validated according to:

- API authentication
- Sender validation (address, IP, server)
- Duplicate request handling
- Recipient validation
- Phone number normalisation
- Date/time validation
- Optional third-party approval

2.7 Workflow Components

Broadcasts

Omni-Channel Broadcasts

Broadcasts may use:

- Single channel
- Multiple channels simultaneously
- Staged / staggered channel escalation

Broadcast Configuration

Each broadcast defines:

- Channels used
- Message content (global or per channel)
- Personalisation tokens
- Recipient sources:
  - Stored contacts
  - Stored distribution groups
  - Dynamic contacts (matching pre-defined activation criteria)
  - API-supplied contacts
  - Calendar-based contacts
  - Contacts associated to system Assets
  - Contact location (as defined in integrated mapping tool)

Broadcast Direction

- 1-Way (no reply handling)
- 2-Way (reply handler enabled)

Advanced Broadcast Features

- Social hours – Messages are only processed between specified times (unless flagged as priority)
- Data overwrite – Sensitive content is overwritten
- Number masking – Set up conversations between external parties without disclosing personal numbers
- Short links – Long URLs are converted to short links
- Web Forms – Configurable web forms are embedded in a message via a short link
- Document management – embed links to stored files to record digital signatures, acceptance of terms and conditions, and acknowledgements denoting that a document has been viewed / read

Delivery Status Handling

Delivery states

- Message has been delivered to recipient's device
- Content has been delivered (i.e. messages has been read / listened to)
- A message has been submitted to the recipient, but delivery is pending and is being retried
- Message has failed to deliver

Status Based Actions
Workflows can:

- Escalate on failure
- Retry delivery
- Switch channels
- Notify third-party systems
- Group recipients by status
- Trigger reports
- Stop or extend workflow runtime

Reply Handling (2-Way Messaging)
Reply handlers allow workflows to react to:

- Any reply
- Keyword-based replies
- Invalid or unexpected replies
- Duplicate replies
- Replies within or outside time windows
- Absence of replies

Reply Based Actions
- Start or continue conversations
- Repeat or escalate messages
- Change channels or recipients
- Update contact records
- Categorise responders / non-responders
- Trigger secondary workflows
- Generate reports

Timed Events & Milestones

Fixed Events
- One-off or recurring scheduled actions

Offset Events
Relative to:

- Activation time
- Variable date/time
- Other milestones

Runtime Control
- Workflow duration limits
- Conditional completion
- Event-based termination
- Milestone cancellation

Calendar Integration

- Activate workflows from calendar events
- Dynamically resolve recipients from events
- API integration with third-party calendars

Workflow Actions

Actions are atomic execution units. Categories include:

- **Form Actions** – Questions, validation, redirects, bookings
- **Variable Operations** – Store, merge, move, count, transform
- **Contact Management** – Load, create, edit, delete contacts
- **Contact Sets** – Static and dynamic grouping
- **Messaging** – Broadcast initiation and message parsing
- **Workflow Control** – Start, stop, restart, forward workflows
- **Milestones** – Schedule, cancel, and manage time events
- **Reporting & Ticketing** – Tickets, reports, SLA tracking
- **Assets** – Asset discovery and contact association
- **Events** – Event creation, correlation, and closure
- **API Integration** – External system integration
- **Data Extraction** – JSON and structured data parsing
- **AI Actions** – AI-assisted analysis and content generation

Please refer to Workflow Actions Reference at Appendix B Schedule 1 for detailed Action definitions.

Workflow Conditions

Conditions determine whether actions execute. Supported condition types include:

- Phone number validation
- Numeric comparisons
- Contact membership and attributes
- Trigger channel checks
- Text and keyword matching
- Variable comparisons
- JSON structure validation
- Date/time and business hours
- Delivery status checks
- Milestone state checks
- Form response validation
- Broadcast success
- Escalation availability
- Recipient counts
- Ticket existence and state

Conditions may:

- Combine multiple rules
- Store matched outputs in variables

- Invert logic where required

Please refer to Workflow Conditions Reference at Appendix B Schedule 2 for detailed Condition definitions.

2.8 Integration & Extensibility

APIs

- Custom inbound and outbound APIs
- HTTP requests with full payload control
- Authentication profiles
- Response parsing and error handling

Third-Party Systems

- CRM
- Service desks
- Asset systems
- Calendars
- Monitoring platforms

2.9 Security, Governance & Access Control

- Role-based access control (RBAC)
- Environment separation
- Workflow editing vs execution permissions
- Audit logging
- Data masking and overwrite
- White labelling for branding consistency

2.10 Non-Functional Considerations

- Scalable, event-driven execution
- Parallel workflow threads
- High availability messaging
- Internationalisation and localisation
- Compliance with messaging regulations (opt-in, data handling)

---

3 boomLogic API Connections

3.1 Overview

The boomLogic UI provides access to configurable API services that enable external systems to securely integrate with, trigger, and exchange data with workflow projects, components, and tasks built within the boomLogic platform. API Connections allow public or partner systems to invoke internal logic, send messages, or integrate third-party and SaaS platforms using secure, managed credentials and structured data mapping.

All integrations are managed through a user interface and protected using encrypted credentials and access controls. The service supports low-code and no-code integration patterns suitable for public sector use cases, including event-driven automation, system interoperability, and secure data exchange.

3.2 Core API Connection Functionality

An API Connection is a named integration configuration owned by a client (product or service). Each connection defines:

- How external systems authenticate.
- What internal logic is invoked.
- How incoming data is interpreted and mapped.
- How credentials and third-party access are securely stored.
- How usage is monitored and audited.

Connections are reusable, centrally managed, and visible within the Logic UI for configuration, testing, and lifecycle management.

3.3 Supported API Connection Types

Logic API Connections

Purpose

Logic API Connections expose secure HTTP endpoints that allow external systems to trigger internal workflows, components, tasks, or events within the boomLogic platform.

Key Capabilities

- Secure, token-authenticated inbound API endpoints.
- Support for multiple triggers per connection.
- Optional data transformation and mapping.
- Routing to workflows, components, tasks, or events.
- Reusable configuration across multiple integrations.

Functional Behaviour

Trigger Configuration

Logic API Connections use Triggers to define what internal logic is executed when an API request is received. In simple terms, a Trigger answers the question:

“When this API Connection is called, which internal workflow or action should run, and how should the incoming data be handled?”

Each Trigger specifies:

- The internal logic type to invoke (component, task, or event).
- The specific internal resource to execute.
- Optional routing references to support multiple workflows sharing a connection.
- Optional data-mapping configuration.

Incoming HTTP requests are authenticated using an inbound token.

A single Logic API Connection may define one or more Triggers, enabling a single API endpoint to invoke different internal processes.

Data Mapping

Logic API Connections support optional Data Mapping to control how incoming JSON payloads are interpreted before being passed to internal logic. In simple terms, data mapping answers the question:

"How do the fields in the external system's data relate to the inputs expected by our internal logic?"

Two modes are supported:

- **Direct (1:1) mode** – the incoming JSON payload is forwarded unchanged.
- **Mapped mode** – incoming JSON is parsed using a reusable JSON Data Collection and mapped to named internal inputs.

Data Mapping:

- Decouples external payload formats from internal data models.
- Supports nested objects and arrays.
- Is configured per Trigger.

Execution Flow

- An external system calls the Logic API endpoint.
- The inbound token is validated.
- The relevant Trigger is selected.
- Incoming data is optionally mapped.
- The target workflow, component, task, or event is executed.
- The request and outcome are logged.

Typical use cases

- Receiving webhooks from third-party systems.
- Triggering workflows from line-of-business applications.
- Submitting structured data into automation processes.

Logic API Connections and Workflow Integration

Inbound, event-driven integration

Logic API Connections are the primary mechanism for external systems to start or feed data into boomLogic workflows.

How Integration Works

- A Logic API Connection exposes a secure HTTP endpoint.
- One or more Triggers are configured on the connection.
- Each Trigger is linked to a specific workflow component, task, or event.

- When an external system calls the API:
  - The request is authenticated.
  - Incoming data is optionally mapped.
  - The associated workflow logic is executed.

Role of Workflows

- Workflows define the business process that runs when the API is called.
- Inputs to the workflow are populated directly from the API payload or via Data Mapping.
- Workflow steps can include decision logic, data processing, messaging, or outbound API calls.

Typical Workflow Use

- Webhook-driven process initiation.
- External system updates triggering workflow progression.
- Data ingestion into automated processes.

3.4 Third-Party API Connections

Purpose

Third-Party API Connections enable the Logic UI & Workflow Builder to securely connect to external systems and SaaS platforms on behalf of users or workflows.
They provide a managed, reusable configuration for outbound API calls, ensuring credentials, request structure, and data handling are consistent, secure, and centrally governed.

Key Capabilities

Third-Party API Connections support:

- Encrypted storage of API credentials and authentication configuration.
- Definition of base URLs and connection-level defaults.
- Reuse of connection settings across multiple workflows.
- Configuration of request parameters and payload handling.
- Structured handling of request and response data.

Connections are configured via the UI and are only accessible to authorised users within the owning client.

Functional Behaviour

Configuration and credentials

- Each Third-Party Connection references an API Profile.
  - The profile defines:
  - Base API URL.
  - Authentication method (e.g. API key, OAuth).
  - Encrypted authentication values.
- Credentials are decrypted only for authorised management or execution contexts.
- Connections can be tested and validated via the UI before use.

Query Parameters

- Static query parameters automatically appended to requests.
- Commonly used for API versioning, tenant identifiers, or required flags.

Default Content Type

- Defines the default Content-Type header for requests.
- Supports formats such as application/Json and application/x-www-form-urlencoded.

POST Form Parameters

- Defines default form-encoded parameters for POST requests.
- Supports APIs that require form submissions, including legacy systems and OAuth token endpoints.

These defaults ensure consistent and compliant request construction across workflows.

Data Configuration and Data Structures

The Data configuration allows administrators to define Data Structures describing how data is sent to and received from third-party APIs. Data Structures:

- Define expected request and response formats.
- Support nested objects and arrays.
- Provide predictable data models for workflow designers.

This ensures workflows interact with external systems using consistent, well-defined data shapes.

Typical use cases

- Payment gateways.
- CRM or case management systems.
- External data services and SaaS platforms.

Third-Party API Connections and Workflow Integration

Outbound service invocation

Third-Party API Connections are used by workflows to call external systems as part of a process.

How Integration Works

- A workflow includes steps that invoke a Third-Party API Connection.
- The connection supplies:
    - Authentication credentials.
    - Default request settings.
    - Defined data structures.
- The workflow provides request data and receives structured responses.

Role of Workflows

- Workflows decide when and why a third-party API is called.
- Responses from third-party systems can:
    - Drive decision logic.

- Update workflow state.
- Be stored or forwarded to other systems.

Typical Workflow Use

- Creating or updating records in external systems.
- Retrieving reference or validation data.
- Retrieving contact data from an external system to provide workflow recipients
- Integrating with payment, CRM, or case management platforms.

3.5 Nylas Integration

Purpose

Nylas API Connections enable secure access to email, calendar, and contact data using the Nylas integration platform.

Key Capabilities

- OAuth-based grant flow.
- Connection status tracking.
- Secure handling of email account metadata.

Functional Behaviour

Grant Flow and Status Management

- Connections track states such as not connected, connecting, connected, or error.
- Successful authorisation stores a grant identifier for ongoing access.
- Errors are recorded and surfaced to administrators.

Scope Limitations

- Nylas API Connections do not use Triggers.
- Nylas API Connections do not support Data Mapping.
- API structure and data handling are defined by Nylas.

Typical use cases

- Connecting user mailboxes to workflows.
- Automating email-driven processes.

Nylas API Connections and Workflow Integration

Authorised data access and event-driven processing

Nylas API Connections enable workflows to access and respond to email, calendar, and contact data.

How Integration Works

- A Nylas Connection authorises access to a user's mailbox or calendar.
- Workflows can:
  - Read messages or events.
  - Process email content.
  - React to changes or scheduled events.

- Connection status determines availability.

Role of Workflows

- Workflows define how email or calendar data is processed.
- Examples include parsing emails, scheduling actions, or triggering follow-up processes.

Typical Workflow Use

- Email-driven case creation.
- Calendar-based scheduling workflows.
- Automated follow-ups and reminders.

3.6 Messaging / Direct API Connections

Purpose

Provide credentialed messaging-style APIs used by messaging channels or external systems.

Capabilities

- API username generation and management.
- Credential lifecycle management via UI.
- Configuration of Messaging API features
    - Set Default dynamic header
    - Enable default Social Hours start and end times per day
    - Enable data overwrite
- Integration with platform messaging services.

Functional Behaviour

Messaging Integration

Messaging API Connections act as **credentialed gateways** into the messaging subsystem.

- Each connection is linked to a Direct API configuration.
- The connection identifier is used as the Direct API username.
- Creating or updating the connection ensures the Direct API configuration remains synchronised.

Typical use cases

- Sending messages via SMS, email, chat, or other supported channels.
- Integrating external messaging providers or clients.
- Supporting multi-channel communication workflows.

Please refer to a separate Appendix C for a detailed specification of Boomerang's Messaging APIs.

3.7 Common Metadata Fields

The following metadata applies to all API Connection types:

- **Label** – human-readable name.
- **Reference** – short unique identifier.
- **Description** – optional explanatory text.
- **Status** – draft, production, or archived.
- **Client ownership** – enforced for access and lifecycle control.
- **Time zone** – used for consistent logging and scheduling behaviour.

These fields support administration, auditing, and safe configuration management.

3.8 API Lifecycle Management (Create, Update, Delete)

All API Connection types support a common lifecycle:

Create / Update

- Validation of required fields.
- Automatic reference generation if not supplied.
- Type-specific validation during save.
- Configuration updates applied consistently.

Delete

- Ownership validation.
- Removal of associated configuration where applicable.
- Cache invalidation to prevent stale access.

This ensures consistent governance regardless of connection type.

3.9 Security and Credential Handling (Where Applicable)

Across all API Connection types:

- Sensitive values are encrypted at rest.
- Credentials are only decrypted in authorised contexts.
- Access to configuration is restricted to authorised users.
- Connection status controls availability.

While the type of credential varies (token, API key, OAuth grant, etc.), the security principles are consistent.

3.10 Status and Environment Control

All API Connection types support:

- **Draft** status for configuration and testing.
- **Production** status for live use.
- **Archived** status to disable without deletion.

This prevents accidental use and supports safe change management.

3.11 Monitoring, Logging, and "Last Used" Tracking

All API Connection types participate in shared monitoring capabilities:

- Request or usage activity is logged.
- Timestamps are recorded for operational insight.
- “Last used” metrics are available in listings.
- Errors are logged and associated with the connection identifier.

This supports audit, troubleshooting, and capacity planning.

3.12 Client and Ownership Validation

For all API Connection types:

- Connections are strictly client-scoped.
- Requests or usage are validated against client ownership.
- Inactive or disabled clients cannot use connections.

This enforces tenant isolation and data protection.

---

4 Asset Management

4.1 Overview / Purpose

The Assets capability allows organisations to create, manage and relate the operational resources they need to track in boomLogic. An Asset represents any customer-defined entity such as a project, building, vehicle, location group, team base or similar resource.

Assets form a core part of the boomLogic platform and are used across the user interface for asset registers, asset detail views, maps, hierarchy management and linking and reporting of operational events.

The Assets entity is designed for secure, multi-tenant public sector use and ensures that each organisation’s data is kept logically separate.

4.2 Key features

The Assets service provides the following core capabilities:

- Create, update and delete Assets securely
- Store descriptive and classification information for each Asset
- Track current and historical locations
- Assign contacts to Assets
- Link Assets to events
- Create parent / child relationships between Assets
- Search, filter and list Assets, including spatial (map-based) filtering
- View summary counts for related data such as locations, contacts and events

4.3 Asset information

Each Asset can store the following information:

- A unique identifier

- Customer (organisation) identifier
- Name and description
- Address and reference information
- Asset type or category
- Creation and update timestamps

4.4 Managing Assets

Creating and updating Assets

- Assets can be created or updated using a single operation.
- If an identifier is not provided, the system generates one automatically.
- Updates are applied atomically to ensure data consistency.

Deleting Assets

- Assets can be deleted when no longer required.
- When an Asset is deleted, all associated relationships (such as links to contacts, locations and hierarchies) are cleaned up automatically to maintain data integrity.

4.5 Location tracking

- Assets can have one or more associated locations.
- The service supports:
    - A current location
    - Historical locations
    - Time-based queries (for example, “where was this asset at a given time”)
    - Representation of Asset locations in Map view
- Locations can be replaced or added as operational needs change.

4.6 Assigning Contacts

- Contacts can be assigned to one or more Assets.
- Assignments can be replaced or updated without creating duplicates.
- This supports scenarios such as asset owners, managers or responsible officers.

4.7 Asset hierarchies

- Assets can be organised into parent and child relationships.
- This allows customers to model real-world structures such as:
    - Buildings within sites
    - Vehicles within fleets
    - Projects within programmes
- The service prevents circular relationships to ensure hierarchies remain valid.

4.8 Searching, filtering and listing

Assets can be:

- Listed with pagination and sorting
- Searched by name
- Filtered by type or category

- Filtered by related events or hierarchical relationships
- Filtered geographically using map-based polygon searches

This allows users to quickly find relevant Assets, even in large datasets.

4.9 Summary information

For each Asset, the service can provide summary information including:

- Number of associated locations
- Number of assigned contacts
- Number of parent and child Assets
- Number of active events

This supports efficient user interfaces and reporting without requiring additional queries.

4.10 Benefits for public sector organisations

- Provides a single, consistent register for operational assets
- Supports complex organisational and geographic structures
- Improves situational awareness through links to locations and events
- Designed for secure, multi-tenant use across public sector bodies
- Scales to support large asset registers and high user volumes

---

5 Monitoring

5.1 Overview

The Monitoring service provides automated monitoring and alerting for digital services, APIs, and external conditions. It allows organisations to configure monitors that run on a defined schedule, evaluate results, and trigger downstream actions or notifications when conditions are met.

The service supports both uptime and endpoint monitoring and event-based monitoring (such as weather alerts), enabling proactive identification of issues and faster response to incidents.

5.2 What the service does

The Monitoring service continuously checks defined targets or conditions and records their status. When checks run, the service can trigger automated workflows by passing structured variables to other systems.

Typical uses include:

- Monitoring website or API availability
- Validating response codes, timeouts, and content
- Supporting recovery workflows after failures

- Triggering alerts or automated actions based on external conditions (such as weather)

5.3 Monitor types

The service supports two main monitor types:

Ping monitors
Used to check URLs or API endpoints. These monitors perform regular “pings” to verify availability, performance, and response behaviour.

Weather monitors
Used to monitor weather conditions and raise alerts when configured thresholds or rules are met.

5.4 Key features

Scheduling and timing
- Monitors can be configured with optional **start** and **end** times.
- Checks only run while the monitor is active and within its configured time window.
- Each monitor can have one or more schedules defining:
  - Frequency (for example, every 5 minutes)
  - Days of the week
  - Time-of-day windows
  - Specific calendar dates can be excluded so checks are skipped when required.

Ping configuration
Each ping monitor includes at least one check configuration:

- **Liveness check** (mandatory): the primary health check that runs regularly.
- **Recovery check** (optional): used after a failure to confirm recovery under different conditions.

Checks can be configured with:

- Target URL, path, and port
- Timeouts
- HTTP headers
- Expected success response codes
- Optional response body matching rules

Weather configuration
The weather monitor uses official Met Office forecast and ensemble data to provide trusted, forward-looking weather intelligence rather than reactive observations. The monitor allows configurations for:

- **Flexible geographic targeting** - Alerts can be scoped country wide, by region, or by county, enabling monitoring aligned to operational footprints.

- **Multi-day forecast alerting** - Conditions can be evaluated for today up to six days ahead, supporting proactive planning and early warnings.
- **Time-of-day awareness** - Weather conditions can be assessed for daytime, nighttime, or both, enabling context-specific alerting.
- **Rich condition types** - Supports multiple forecast parameters including significant weather, wind speed, wind direction, gusts, visibility, temperature, humidity, and probability of snow.
- **Threshold-based rules** - Alerts trigger when forecast values equal, exceed, or meet defined thresholds, allowing precise control over alert sensitivity.
- **Multiple conditions per monitor** - Users can define and combine several weather conditions within a single monitor.
- **Colour-coded severity** - Conditions can be assigned visual severity indicators to support prioritisation and escalation.
- **Workflow-driven automation**
  When conditions are met, structured alerts trigger automated workflows for notifications, escalations, or operational actions.

Status and lifecycle

- Monitors have a lifecycle state: *draft*, *active*, or *archived*.
- Only active monitors run.
- The system maintains a status for each monitor, including:
  - Last check result
  - Current health state (for example OK or failing)
  - Next scheduled run time
- Next run times are automatically calculated based on the configured schedule.

Triggers and automation

When a monitor runs, it can dispatch triggers to other parts of the system or integrated services.

Triggers include structured variables such as:

- Monitor name, description, and priority
- Current status
- URL checked
- HTTP response code and response body (where applicable)

Users can also define custom variables on a per-project basis to support integration with downstream workflows.

Triggers are processed asynchronously to ensure monitoring checks remain responsive and scalable.

5.5 Security and data protection

- Sensitive configuration values, such as HTTP header values, are encrypted before being stored.
- Encrypted values are only decrypted at runtime when a check is executed.
- Free-text fields are sanitised to prevent injection or content-related issues.

- The service follows secure error handling and logging practices.

5.6 Data handling and persistence

Creation and updates

- Monitors are created and updated using safe “upsert” operations to prevent duplication or conflicts.
- Related configuration (such as API connections) is managed transactionally to avoid partial or inconsistent data.
- Validation is performed on save to ensure required configuration is present and correctly formatted.

Deletion

- Deleting a monitor also removes its associated checks and related configurations in a single transaction.
- This ensures no orphaned or partial data remains.

5.7 Standards and formats

- Date and time values use RFC3339 format (for example: **2026-01-13T15:04:05Z**).
- Scheduling and execution align checks to consistent minute boundaries.

5.8 Service limitations

- Ping monitors must include exactly one liveness check.
- Only one recovery check is permitted per monitor.
- Monitoring runs only when the monitor is active and within its configured schedule.
- If required system variables are missing from a trigger configuration, monitoring will continue but a warning may be logged.

5.9 Service management and support

Monitoring visibility

Users can view:

- Monitor configuration
- Current and historical status
- Upcoming scheduled run times

5.10 Integrating Monitoring with Logic Workflows

Overview

Monitoring integrates directly with the Logic workflow service. When a monitor runs or its status changes, it can automatically start Logic workflows by passing monitoring results as workflow inputs.

This enables monitoring outcomes to drive automated actions without manual intervention.

How the integration works

1. A monitor check completes or the monitor's status changes (for example, it becomes failing or starts recovering).
2. The Monitoring service prepares one or more triggers, grouped by Logic project.
3. For each project, the service packages:
    - The monitor details
    - The current monitor status
    - A set of trigger variables mapped to workflow inputs
4. The trigger is placed onto a background processing queue.
5. A Logic worker retrieves the trigger and starts one or more workflow runs using the provided inputs.

All workflow execution is handled asynchronously to ensure monitoring remains responsive and scalable.

Workflow inputs and trigger variables

System generated variables

The Monitoring service automatically generates standard variables that can be used as Logic workflow inputs, including:

- Monitor status
- URL checked
- HTTP response code and response body
- Monitor name, description, and priority
- Associated API name (if applicable)

These values are resolved at runtime and passed into workflows in a structured format.

User defined variables

Users can define custom variables on a per-project basis. These values are passed unchanged into Logic workflows and can be used for:

- Notification destinations
- Escalation rules
- Workflow-specific parameters

Where multiple values are provided, the workflow engine can process them according to the workflow's design.

Workflow execution behaviour

- Trigger variables are mapped directly to workflow input arguments.
- Logic workflows receive inputs that match their defined input schema.
- If required input values cannot be resolved, the trigger job is logged and handled according to configured error-handling behaviour.
- Monitoring continues independently of individual workflow execution outcomes.

Typical use cases

Automated incident response

- A service endpoint fails a health check.
- Monitoring triggers a Logic workflow.
- The workflow sends alerts, creates tickets, or runs remediation steps.

Recovery validation

- A recovery check confirms a service is responding normally.
- A workflow records recovery events or closes incidents.

Event driven automation

- A weather condition is met.
- Monitoring triggers workflows that notify stakeholders or update systems.

---

6 Events

6.1 Overview

The CPaaS platform provides an Events and Incident Management capability that enables organisations to create, manage and communicate operational events, incidents and alerts through a secure, web-based interface.

Events can be created:

- Manually by authorised users via the user interface
- Automatically based on alerts generated by Monitoring tools within the CPaaS platform or events triggered by other external systems or resources.
- Via configurable Logic workflows

Events are a core capability of the service used to record, track, and manage incidents, alerts, or notifications. Events provide real-time visibility of operational issues and support coordinated incident response, stakeholder communications and audit reporting. notifications.

6.2 Creating an Event Manually

Authorised users can create Events manually from the Events page or via the Map view (where the event is assigned to a specified location or geographical area on the Map view). Users are then guided through a step-by-step user interface to complete the Event details. When creating an Event manually, users can:

- Select the Event type (Warning, Alert or Notification)
- Define Event and incident details, including:
  - Event name and reference
  - Location (optional) – allows the Event to be displayed on the Map view
  - Description and impact
  - Severity level (Low, Medium, High, Critical)
  - Start and end date/time

- Associate the Event with one or more Assets
- Create custom fields for the event

Asset association and contact automation

Events can be associated with system-managed Assets, such as services, buildings, vehicles or infrastructure.

Assets can have Contacts assigned to them. When an Event is associated with an Asset:

- Contacts linked to the affected Asset can be automatically included in communication distribution lists
- This helps ensure relevant stakeholders are notified quickly and consistently

Assets can be selected from a list or map-based interface.

Communications and engagement

The service supports both automated and manual communications throughout the Event lifecycle. Communications can be sent via:

- SMS
- Email
- Voice messaging
- WhatsApp
- RCS

Authorised users can create and send communications manually from the user interface at any point during the Event lifecycle. When creating an Event from the interface, recipients of communications can be added by:

- Selecting system contacts or distribution groups
- Adding a list of contact addresses (e.g. telephone numbers or Email addresses)
- Select a pre-configured Logic workflow to manage communication processes for the Event. This allows:
    - Automated communications to be triggered as part of a manually created Event
    - Consistent engagement and escalation processes to be applied
    - A combination of manual incident management and automated behaviour

Authorised users can create and send communications manually from the user interface or connect the event to a Logic workflow at any point during the Event lifecycle.

All communications, automated or manual and any outputs resulting from those communications (e.g. stakeholder responses) are recorded in the Event timeline.

6.3 Automated Events

Events can also be created automatically without user intervention.

Monitoring-triggered Events

Events can be created automatically when Monitoring tools within the CPaaS platform raise alerts, such as:

- Service availability issues
- Performance threshold breaches
- Infrastructure or operational alerts

When a Monitoring alert is triggered:

- A connected Logic workflow creates an Event automatically
- Automated communications and actions can be executed
- The Event appears immediately on user dashboards for real-time visibility
- The Event appears on the Map view for Events that have an associated location. The Map view provides access to the Events details and controls to manage the Event, including accessing the Event timeline, issuing Event updates, closing the Event.

External system-triggered Events

Events can also be created as a result of triggers from external platforms or systems. In this scenario:

- An external system triggers a connected Logic workflow (for example via API or integration)
- The workflow automatically creates an Event
- Automated communications and escalation rules can be applied
- The Event appears immediately on user dashboards for real-time visibility

This allows organisations to integrate third-party systems into their incident management and communications processes.

6.4 Event management and updates

Events can be managed using a combination of automated workflow behaviour and manual user actions. Authorised users can:

- Update severity levels
- Record internal progress updates (for example triage status or expected resolution times)
- Publish updates to impacted stakeholders
- Close Events once resolved

Events are accessible via a central dashboard to support real-time operational oversight.

6.5 Stakeholder interactions

Interactions with stakeholders in response to Event-related communications are captured automatically. Examples include:

- Engineers responding to monitoring alerts
- Stakeholders accepting jobs or providing progress updates
- Responses to automated or manual notifications

All interactions are recorded in the Event timeline.

6.6 Incident timeline and audit trail

Each Event maintains a comprehensive incident timeline that records:

- Manual and automated Event creation
- Monitoring alerts and external system triggers
- Workflow actions and outputs
- Automated and manual communications
- Stakeholder interactions and responses
- User updates, severity changes and closure
- Ticket associations and correlations

All entries are time-stamped and attributed to a user, system process or external interaction.

This provides a complete audit trail to support SLA compliance, post-incident reporting and root cause analysis.

6.7 Ticketing and event correlation

Events can be associated with tickets to consolidate related incidents and information. Ticket correlation supports:

- Linking Events to service management processes
- Managing complex or multi-stage incidents
- Maintaining a single view of incident activity and communications

6.8 Access control

Event creation, updates, communications and closure are controlled through role-based access permissions.

---

7 Reporting & Dashboards

7.1 Overview

The CPaaS platform provides comprehensive reporting and dashboard capabilities designed to deliver real-time visibility, operational insight, and performance transparency across all messaging and workflow activities. Interactive dashboards present key metrics such as message volume, delivery status, channel performance, workflow execution, and system health, enabling users to quickly assess outcomes and identify trends at a glance.

Reporting capabilities support both standard and customizable reports, allowing users to analyse campaign effectiveness, inbound and outbound interactions, API usage, and event activity over configurable time periods. Reports can be filtered by channel, asset, campaign, workflow, or integration, providing granular insight into communication performance and operational efficiency. Data can be exported or integrated with external analytics and business intelligence tools to support compliance, auditing, and strategic decision-making.

Together, dashboards and reporting empower operational, technical, and business teams with a single source of truth for monitoring performance, troubleshooting issues, measuring ROI, and continuously optimizing communication strategies across the CPaaS application.

7.2 Types of Reporting Data

Messaging Reports

- **Message Delivery** – Tracks messages by status (e.g. Delivered, Failed etc) and channel (SMS, email, voice, etc.).
- **Message Volumes** – Displays message volumes over time, broken down by channel, campaign, asset, or application.
- **Error & Failure Report** – Highlights delivery failures, error codes, and retry outcomes.

Campaign & Broadcast Reports

- **Broadcast Campaign Performance Report** – Analyses reach, delivery rates, engagement, and opt-outs for broadcast messaging.
- **Inbound Campaign Report** – Summarises inbound message volumes, keywords, response rates, and automated actions triggered.
- **Conversion & Response Report** – Measures user responses and downstream actions resulting from campaigns.

Workflow & Automation Reports

- **Workflow Execution Report** – Tracks workflow runs, success/failure rates, execution time, and branching paths.
- **Workflow Status Report** – Provides insight into workflow status, completion rates and Actions consumed
- **Event Trigger Report** – Shows which events triggered workflows and how frequently.
- **Automation Efficiency Report** – Compares automated versus manual interactions to highlight efficiency gains.

API & Integration Reports

- **API Usage Report** – Details API call volumes, endpoints used, response times, and error rates.
- **Integration Health Report** – Monitors the status and performance of third-party and internal integrations.
- **Authentication & Access Report** – Tracks API keys, tokens, and usage by application or client.

Inbound & Contact Interaction Reports

- **Inbound Interaction Report** – Summarises inbound messages, calls, and responses by channel, asset, or contact.
- **Contact Engagement Report** – Measures interaction frequency and responsiveness.
- **Opt-In / Opt-Out Report** – Tracks consent status changes and compliance-related activity.

Asset Reports

- **Asset Communication Report** – Shows all messaging and interactions associated with a specific asset.
- **Asset Performance Report** – Compares communication volume and outcomes across assets or asset types.
- **Assigned Contact Report** – Lists contacts associated with assets and their communication activity.

Monitoring, Alerts & Reliability Reports

- **System Health & Uptime Report** – Provides visibility into platform availability and service performance.
- **Alert History Report** – Tracks triggered alerts, severity, resolution times, and outcomes.
- **Incident & Ticket Report** – Summarizes support tickets, root causes, and resolution metrics.

Event Reports

- **Event Timeline Report –** Provides a record of Event actions and status milestones in a chronological timeline.
- **Event Communications Report –** Provides a summary of communications and engagement by Event.
- **Event Activation Report** – Provides an overview of Events by activation method and activation source.

Compliance & Audit Reports

- **Message Audit Trail Report** – End-to-end traceability of message lifecycle events.
- **Data Access & Change Log Report** – Tracks configuration changes, user actions, and administrative updates.

Financial & Usage Reports

- **Usage & Consumption Report** – Tracks message counts, Workflow Actions consumed, API usage, and feature consumption.
- **Cost Allocation Report** – Breaks down usage and costs by asset, campaign, department and User
- **Trend & Forecast Report** – Identifies usage trends to support planning and budgeting.

8 Broadcast Messaging Interface

A specification for the Broadcast Interface provided as part of Boomerang's CPaaS Messaging & Workflow Platform is provided at Appendix B.

---

9 Messaging API

A specification for the Messaging API provided as part of Boomerang's CPaaS Messaging & Workflow Platform is provided at Appendix C.

---

10 Email-to-SMS and Voice

A specification for Email-to-SMS and Voice provided as part of Boomerang's CPaaS Messaging & Workflow Platform is provided at Appendix E.

---

11 Inbound Communications

A specification for Inbound Communications provided as part of Boomerang's CPaaS Messaging & Workflow Platform is provided at Appendix F.

Appendix A – Schedule 1: Workflow Actions Reference

1 Overview

Workflow Actions are the atomic execution units within a boomLogic workflow.
Actions are executed when:

- A workflow is activated
- A condition evaluates to true
- A milestone is reached
- An inbound event (reply, delivery status, form submission, API event) occurs

Actions may:

- Modify workflow state
- Send communications
- Interact with contacts, assets, tickets, and events

- Integrate with external systems
- Control workflow execution

Actions execute within either:

- Main workflow thread (shared state)
- Current execution thread (parallel execution)

Legend

- **Action Type**: System identifier used in workflow configuration
- **Category**: Functional grouping
- **Purpose**: What the action does
- **Inputs / Configuration**: Key inputs, variables, or options
- **Outputs / Effects**: What the action produces or changes
- **Typical Use Cases**: Common scenarios

2 Actions Defined

Form Actions

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases
Set Form Question	Displays a question in a web form	Question text, type, options	Renders UI element only	Surveys, data capture
Reject Form	Rejects form submission	Static rejection message	Submission rejected, user notified	Validation failures
Form Redirect	Redirects user after submission	URL (static or variable)	Browser redirect	Thank-you pages
Assign Form Reply To Variable	Stores form answers	Question UUID, variable, operation	Variable updated	Capture responses
Create Event Form	Creates booking from form	Form fields, calendar config	Event created	Appointment booking

Variable Operations

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases

Store Reply	Stores inbound message reply	Target variable, operation	Variable populated	Capture SMS/email replies
Update Variable	Stores arbitrary data	Data value, variable	Variable updated	Token storage
Set Counter	Performs arithmetic	Number source, operation	Numeric variable updated	Quotas, counters
Merge Variables	Copies one variable to another	Source & destination variables	Variable merged	Combine lists
Move Variables	Moves one item	Source, destination	Item moved	Queue processing
Delete Variable	Deletes one item	Variable, position	Item removed	Stack/queue cleanup
Subtract Variables	Removes matching values	Two variables	Filtered variable	Exclude responders
Unique Variables	Deduplicates variable	Variable	Unique values only	Clean contact lists
Started By Variable	Stores workflow starter	Contact variable	Starter stored	Audit, tracking
Recipient Variable	Stores responder	Contact variable	Recipient stored	Response handling
Time Zone From Location	Derives time zone	Phone/location variable	Time zone variable	Local scheduling
Get Filenames	Extracts filenames	File variable	Text variable	Document lists

Contact Set Management

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases
Store Input To Dynamic Contact Set	Adds contacts to context	Contact variable	Context updated	Runtime audiences

Add Starter To Contact Set	Adds starter to group	Group UUID	Group updated	Opt-in tracking
Add Responder To Contact Set	Adds responder	Group UUID	Group updated	Engagement lists
Remove Starter From Contact Set	Removes starter	Group UUID	Group updated	Opt-out
Remove Responder From Contact Set	Removes responder	Group UUID	Group updated	Data hygiene
Remove All From Contact Set	Clears group	Group UUID	Group emptied	Reset
Add Contact to Group	Adds contacts	Contact variable	Group updated	Bulk management
Remove Contact From Group	Removes contacts	Contact variable	Group updated	Bulk removal
Add Dynamic Contact Set To Contact Set	Context → static group	Group UUID	Group populated	Persist audience
Remove Dynamic Contact Set From Contact Set	Context → removed	Group UUID	Group updated	Cleanup

Message & Communication

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases
Start Broadcast	Sends outbound messages	Template, channels, recipients	Messages sent	Notifications
Set Dynamic Comms	Sets channel preferences	Escalation rules	Runtime comm config	Channel fallback
Extract Text – Input Argument	Parses inbound text	Delimiters, CSV, validation	Variable populated	Structured replies

Workflow Control

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases

Start Runtime	Starts workflow instance	Workflow UUID	New runtime	Child workflows
Restart Runtime	Restarts workflow	Restart type	Workflow restarted	Retries
Stop Runtime	Stops workflow	None	Runtime terminated	Completion
Stop Process	Stops all workflows	None	Process terminated	Emergency stop
Forward Event	Routes event	Target workflow	Event forwarded	Modular flows

Milestone Management

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases
Set Milestone	Schedules milestone	Date/time or offset	Workflow paused	Delays, reminders
Cancel Milestone	Cancels milestone	Milestone ID	Workflow resumes	Abort waits

Reporting & Ticketing

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases
Create Ticket	Creates ticket	Topic, description	Ticket created	Incidents
Set Ticket	Sets ticket context	Ticket reference	Context updated	Linking
Unset Ticket	Removes ticket	None	Context cleared	Cleanup
Set Ticket Status	Updates ticket status	Status	Ticket updated	Resolution
Create Reporting Entry	Creates report entry	Template, fields	Entry created	Auditing
Load Reporting Entry	Loads report entries	Filters	Variable populated	SLA checks

Asset Management

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases
Assign Assets To Variable	Loads assets	Filters, relationships	Asset variable	Infrastructure alerts
Assign Asset Contacts to Variable	Loads asset contacts	Asset variable	Contact variable	Notify owners

Event Management

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases
Create Event	Creates event	Title, severity	Event created	Incidents
Close All Events	Closes events	Ticket or variable	Events closed	Resolution
Find Event By Ticket	Finds events by ticket Id	Ticket reference	Event variable	Correlation

API Integration

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases
Make API Request	Executes HTTP request	Method, payload, headers	Response variables	CRM, calendars

Data Extraction

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases
Extract Data From Structure	Extracts data from a pre-defined data structure	JSON path	Variable populated	API parsing

AI Actions

Action Type	Purpose	Inputs / Configuration	Outputs / Effects	Typical Use Cases
AI Prompt	Executes AI prompt	Prompt text, files	AI response stored	Summaries, analysis

Notes

- All actions support thread selection (main vs current) where applicable
- Most actions support error capture and continuation
- Variable format compatibility must be enforced at design time
- Actions execute only when associated conditions evaluate to true

Appendix A – Schedule 2: Workflow Conditions Reference

1 Overview

Workflow Conditions are the logical evaluation units within a boomLogic workflow. They determine whether a rule or action should execute based on data, events, time, or system state. Conditions do not perform actions themselves, instead they act as decision gates, ensuring that workflow execution follows the correct logical path.

2 Conditions Defined

Legend

- **Condition Type**: System identifier used in workflow rules
- **Category**: Functional grouping
- **Purpose**: What the condition evaluates
- **Inputs / Configuration**: Key inputs, operators, and options
- **Evaluation Result**: When the condition evaluates to TRUE
- **Typical Use Cases**: Common scenarios

Phone Number Validation

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Validate Phone Number	Validates phone numbers	Number variable, country codes, number types, operator	At least one number meets all validation rules	Mobile-only SMS, country filtering

Number Comparison

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Compare Number	Compares numbers or counts	Number(s), operator, compare-type	Numeric comparison passes	Quotas, thresholds, limits

Contact Membership Checks

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Check Contact In Variable	Checks for a contact in a variable	Contact variable	Contact found	Conditional routing

Check Contact In Group	Checks for contact in a group	Contact set UUID	Contact is member	Role-based flows
Contact Context	Checks contact in context	None	Contact in runtime context	Dynamic audiences
Check Starter In Variable	Checks workflow starter	Variable	Starter found	Permission checks
Check Starter In Group	Checks starter in group	Contact set UUID	Starter is member	Admin flows
Check Starter In Context	Checks starter in context	None	Starter in context	Audit
Check Recipient In Variable	Checks recipient	Variable	Recipient found	Response routing
Check Recipient In Group	Checks recipient in group	Contact set UUID	Recipient is member	Escalation
Check Recipient In Context	Checks recipient in context	None	Recipient in context	Conversation tracking

Contact Field Value Checks

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Check Contact Has Value	Checks contact field value	Field UUID, value	Any contact matches	VIP handling
Check Starter Has Value	Checks starter field	Field UUID, value	Starter matches	Privileged access
Check Recipient Has Value	Checks recipient field	Field UUID, value	Recipient matches	Segmentation
Check Context Has Value	Checks context contacts	Field UUID, value	Any context contact matches	Bulk decisions

Trigger Channel

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Trigger Channel	Identifies activation channel	Channel(s): SMS, Email, API, Manual	Trigger channel matches	Channel-specific flows

Text Comparison (Inbound Content)

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Reply Message	Compares reply text	Operator, value(s)	Reply matches condition	Yes/No replies
Email Or SMS Body	Compares message body	Operator, value(s)	Body matches	Keyword parsing
Email Subject	Compares subject	Operator, value(s)	Subject matches	Thread routing

Variable Text Comparison

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Variable Text	Compares variable content	Variable UUID, operator, value(s)	Variable comparison passes	Decision logic

Data Presence

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
JSON Data	Checks JSON key existence	JSON path	Key exists	API response checks

Date & Time Conditions

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Compare Date Time	Compares date/time	Operator, datetime, time zone	Time comparison passes	Scheduling
Date Time Business Hours	Checks business hours	Business hours UUID	Time is within hours	Social hours

Delivery Status

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Check Status	Checks message status	Status group	Status matches	Escalation

Milestone Conditions

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Check Milestone Reached	Checks milestone reached	Milestone label	Label matched	Workflow branching
Check Milestone Pending	Checks pending milestone	Milestone label	Pending exists	Reminder control

Form Reply Conditions

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Check Form Reply	Evaluates form answers	Question UUID, operator	Answer matches	Surveys, bookings

Broadcast Success

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Check Broadcast Success	Checks broadcast outcome	Rule UUID	Any message processed	Retry logic

Escalation Availability

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Check Escalation Available	Checks escalation paths	None	Further channel available	Multi-channel escalation alerts

Recipient Count

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Recipient Count	Compares recipient count	Recipient type, count	Comparison passes	Safety checks

Ticket Conditions

Condition Type	Purpose	Inputs / Configuration	Evaluation Result	Typical Use Cases
Ticket Exists	Checks ticket existence	Ticket reference	Ticket exists	Idempotency
Ticket Assigned	Checks ticket is assigned	None	Ticket associated	Workflow gating
Check Ticket Topic	Checks topic / status associated to a ticket	Topic UUID, status	Match found	SLA logic

General Behaviour Notes

Aspect	Description
Operators	Equality, inequality, text matching, ranges, existence
Boolean Inversion	All conditions support inversion
Output Variables	Some conditions store matched values
Threading	Conditions support main/current thread
Multi-value Handling	ANY-match logic unless specified

Summary

Workflow Conditions provide the decision-making framework for boomLogic workflows.
They enable workflows to:

- React intelligently to user behaviour
- Enforce validation and compliance
- Branch dynamically based on time, data, and events
- Control escalation and completion logic

Appendix B - Functional specification for Broadcast Messaging

1 Overview

Broadcast is a secure, multi-channel communications service that enables organisations to design, manage and send messages to large or targeted audiences. It supports email, SMS voice, RCS and WhatsApp messaging from a single system, with built-in personalisation, validation and auditability.

The service is project-agnostic and modular, meaning message templates can be reused across different campaigns, projects or schedules, or created and sent immediately as one-off communications. Broadcast is designed for high-volume and regulated environments, supporting client isolation, permissions, validation and delivery tracking.

Broadcast can be used to:

- Create reusable message templates
- Send immediate or scheduled communications
- Personalise messages using recipient data
- Support one-way notifications or two-way conversations
- Track delivery, replies and outcomes

---

2 Core Messaging Capabilities

2.1 Multi-Channel Messaging

Broadcast supports the following channels:

- SMS
- Email
- Voice
- RCS
- WhatsApp

2.2 Channel-Specific Message Variants

Within a single broadcast, each channel is defined as a **separate message variant**. This allows:

- Content to be tailored to channel constraints
- Different formatting or wording per channel
- Channel-specific sender details (e.g. email subject lines)

For example, an email may contain detailed instructions, while an SMS variant contains a short summary and link.

2.3 Channel Selection and Delivery Rules

Broadcast can determine which channel(s) to use for each recipient based on:

- Available contact details (e.g. email address, phone number)
- Configured delivery preferences
- Channel selection rules defined in the broadcast

This ensures messages are only sent through channels that are valid for each recipient.

2.4 Consistent Personalisation Across Channels

Personalisation tokens are shared across channel variants:

- The same contact data can be used to personalise messages
- Token validation ensures all required data exists before sending
- Defaults can be applied where channel constraints require simplified content

This ensures consistency while respecting channel limitations.

2.5 One-Way and Two-Way Communication

Broadcast supports both:

- **One-way communications** (notifications and announcements)
- **Two-way communications** (where recipients can reply)

For two-way flows, configurable **handlers** define how replies and delivery statuses are processed, for example:

- Creating support tickets
- Triggering workflows or webhooks
- Storing replies for audit and review

Two-Way Interaction by Channel

For supported channels:

- Recipients can reply directly to messages
- Replies are routed back to the originating broadcast transaction
- Handlers define how responses are processed

Different channels can have different reply handling behaviours within the same broadcast.

Handlers for Delivery Receipts and Responses

Handlers enable Broadcast to receive, interpret and act on inbound information generated after a message is sent. This includes both:

- **Delivery Receipts (DRs)** – automated status updates from delivery providers
- **Recipient Responses** – replies sent by recipients (for example, SMS replies)

Handlers define what should happen when these inbound events occur, allowing organisations to move beyond one-way notifications and support interactive or auditable communication flows.

Delivery Status Handlers

Delivery receipts are **status notifications** sent automatically by delivery providers to confirm what happened to a message, such as:

- Delivered
- Read
- Failed
- Expired
- Answered
- Rejected

When a delivery receipt is received:

- The receipt is matched to the originating broadcast and recipient
- The configured handler is invoked
- The status is recorded and processed according to the handler rules

Typical handler actions include:

- Updating delivery status for reporting
- Forwarding to an Email address
- Connecting to a boomLogic workflow Project. For example, to:
    - Trigger failover to a different communication channel for non-delivered messages
    - Forward the DR to a webhook
    - Produce and distribute a report of messaging by status
    - Etc.

Reply Handlers

Responses are **messages sent back by recipients**, typically through channels that support replies (such as SMS). Responses may include:

- Free-text replies
- Keywords (e.g. “YES”, “NO”, “HELP”)
- Automated acknowledgements

When a response is received:

- The system identifies the broadcast and recipient
- The response content is passed to the configured handler
- The handler determines the appropriate action

Typical handler actions include:

- Forwarding to an Email address
- Triggering a pre-configured auto-reply message
- Connecting to a boomLogic workflow Project. For example, to:
    - Trigger failover to a different communication channel where for non-responded messages (after a specified time)
    - Trigger follow-up communication workflows
    - Creating a task, ticket or case in another system

- Forward the response to a webhook
- Produce and distribute a report of responders / non-responders
- Etc.

2.6 Scheduling Broadcast Sends

Scheduling allows broadcasts to be sent automatically at defined times or intervals, without requiring manual intervention. This ensures messages are delivered consistently, on time, and in accordance with operational, regulatory or service requirements. Scheduled sending integrates fully with Broadcast's validation, personalisation, audit and delivery capabilities.

Types of Scheduling Supported

Broadcast supports multiple scheduling patterns, including:

- **One-off scheduled sends**
  A broadcast is sent once at a specific future date and time.
- **Recurring sends**
  Broadcasts can be configured to repeat at regular intervals, such as daily, weekly or monthly.
- **Event- or project-driven schedules**
  Broadcasts may be triggered by external workflows, projects or orchestration rules.

These options allow organisations to automate both routine and time-critical communications.

2.7 Example Use Cases

- **Service Outage Alert** - Send an SMS and voice message for immediate attention, followed by a detailed email.
- **Appointment Reminder** - Use SMS for reminders and email for confirmation details.
- **Emergency Communication** - Deliver urgent messages across all available channels to maximise reach.
- **Automated Follow-Ups** -Trigger additional messages based on delivery status or response content.
- **Service Desk Integration** - Convert replies into support tickets or cases automatically.
- **Planned Maintenance Notices** - Schedule advance notifications and follow-up reminders.

---

3 Message Templates and Ad-Hoc Sends

Broadcast operates in two modes:

3.1 Template mode

- Messages are saved as reusable templates.
- Templates can be cloned and adapted for new use cases.
- Useful for repeat communications such as service updates or alerts.

3.2 Ad-hoc send mode

- Messages are created and sent immediately without being saved.
- Suitable for one-off or urgent communications.

Both modes use the same validation, security and delivery mechanisms.

---

4 Rich Content and Editor Support

4.1 Overview

Rich Content and Editor Support enable users to create, manage and send professionally formatted messages across multiple channels while maintaining consistency, accessibility and reliability. The editor allows content to be authored once, reviewed visually, and then rendered accurately at send time.

The service is designed to support both ease of use for non-technical users and robust validation for large-scale communications.

4.2 Rich Text Editing

The editor supports rich text content, including:

- Formatting (headings, bold, italics, lists)
- Links and call-to-action elements
- Structured layouts suitable for email and other channels

Content is stored in a structured format, allowing it to be:

- Safely edited over time
- Rendered consistently across devices
- Validated before sending

4.3 Channel-Appropriate Rendering

Each message variant is rendered according to its delivery channel:

- WhatsApp, RCS and Email content is rendered as HTML with appropriate fallbacks
- SMS content is rendered as plain text and length-checked
- Voice content is rendered as script text suitable for text-to-speech or recorded playback

This ensures content is fit for purpose without requiring users to manage low-level formatting.

Plain Text Fallbacks

Where required (e.g. email delivery):

- A plain text version of the message is stored or generated

- This improves accessibility and compatibility with different clients
- Validation ensures at least one valid representation exists

4.4 Short Links and Controlled Access

Short Links and Controlled Access enable organisations to include secure, trackable and user-friendly links within Broadcast messages. Long or complex URLs are replaced with short links that reduce the message character count. Additional security controls include:

- Expiry dates – link expires on set date
- Usage limits – limit the number of times a link is accessed
- Password protection – password required to access the link

This allows organisations to control access to linked content and track engagement.

Tracking and Analytics

Short link usage is tracked, providing insight into:

- Whether recipients accessed linked content
- How often links were visited
- When access occurred (subject to retention policies)

This information supports reporting, evaluation and service improvement.

Example Use Cases

Service Portal Access - Send an SMS containing a short link to a secure service page that expires after 48 hours.

Document Distribution - Share a link to sensitive guidance with password protection and limited usage.

Campaign Tracking - Measure engagement by tracking how many recipients accessed linked content.

4.5 Tokens and Personalisation

The editor is token-aware:

- Users can insert personalisation tokens directly into content
- Tokens represent recipient-specific data (such as names or references)
- The editor tracks which tokens are used

Before sending:

- Tokens are validated against available data fields

4.6 Preview Before Sending

Rich content can be previewed:

- With example or test data

- In channel-specific formats
- Before saving or sending

This reduces errors and increases confidence in high-impact communications.

4.7 Separation of Editing and Sending

The system separates:

- **Editor state** (used for authoring and preview)
- **Rendered content** (used for actual sending)

This ensures:

- Editing remains flexible and reversible
- Sending uses a stable, validated representation
- Content can be reused safely across multiple sends

4.8 Consistent Rendering at Scale

For bulk and scheduled sends:

- Content is rendered programmatically for each recipient
- Personalisation tokens are replaced with recipient-specific values
- Rendering is deterministic, ensuring consistent results

This approach supports large-scale communications without sacrificing accuracy.

4.9 Accessibility and Content Quality

Rich Content and Editor Support help organisations meet accessibility and quality standards by:

- Supporting structured content
- Enabling clear formatting and hierarchy
- Allowing alternative text and plain text versions

4.10 Example Use Cases

Policy Announcement - Create a well-formatted email with headings and links, with a simplified SMS version derived from the same content.

Transactional Message - Use tokens to personalise rich email content while maintaining a consistent structure.

Recurring Communications - Update a template once and reuse it across multiple scheduled sends.

---

5 Recipient Management

Broadcast supports multiple ways to define recipients:

- **Contact lists** (managed by an integrated contacts service)
- **Groups** of contacts
- **File imports** (e.g. CSV uploads) with configurable header mapping
- Explicit inclusion or exclusion of contacts or groups

Recipients can be filtered and combined dynamically at send time.

5.1 Dynamic Grouping of Contacts

Dynamic grouping allows Broadcast to target recipients based on live rules and attributes, rather than relying solely on fixed, manually maintained contact lists. Instead of storing a static snapshot of recipients, a dynamic group defines who should receive a message at the moment it is sent, based on current contact data.

This ensures messages are always sent to the most accurate and up-to-date audience, reducing manual maintenance and the risk of sending messages to the wrong recipients.

What Is a Dynamic Group?

A dynamic group is a rule-based definition of contacts, rather than a fixed list. The rules are evaluated at send time using contact data held in the contacts service.

Examples of dynamic group rules include:

- Contacts with a specific role or classification
- Contacts linked to a particular organisation or location
- Contacts with certain preferences or consent flags
- Contacts whose status has changed recently (e.g. active, suspended)
- Contacts matching combinations of multiple criteria

The actual recipients are calculated each time a broadcast is executed, not when the broadcast is created.

How Dynamic Groups Are Used in Broadcast

Broadcast can reference one or more dynamic groups when defining its audience. These groups are resolved at send time as part of the recipient-resolution step.

Dynamic groups can be:

- Included as part of the main audience
- Combined with static contact lists
- Excluded (ignore groups) to suppress certain recipients

This allows precise audience control, even in complex scenarios.

Inclusion and Exclusion Logic

Broadcast supports both **include** and **exclude** rules for dynamic groups:

- **Include groups**
  Contacts that match the group rules are eligible to receive the message.

- **Exclude (ignore) groups**
  Contacts that match exclusion rules are explicitly removed from the final recipient set, even if they also appear in an included group or list.

This approach supports common governance needs such as:

- Suppressing opted-out contacts
- Excluding internal users from public communications
- Removing recipients involved in other active campaigns

Example Use Cases

Policy Update Notification - Send a message to all contacts with an “active” status and a specific service entitlement, excluding those who have opted out.

Operational Alert - Notify all on-call staff in a particular region, based on current rota and role assignments.

Recurring Communications - Schedule a weekly broadcast to all contacts meeting certain eligibility criteria, without needing to update recipient lists manually.

5.2 Contact Lists

Contact lists provide a managed, reusable way to define audiences for Broadcast communications. A contact list represents a named collection of contacts held within the contacts service and can be reused across multiple broadcasts, projects or schedules.

Unlike dynamic groups, which are rule-based and evaluated at send time, contact lists typically represent a curated or pre-defined audience, offering predictability and control where a fixed or semi-fixed recipient set is required.

How Contact Lists Are Used in Broadcast

Each broadcast can reference one primary contact list as its core audience. When a broadcast is sent, Broadcast:

- Requests the list membership from the contacts service
- Applies any additional inclusion or exclusion rules
- Deduplicates the resulting contacts
- Proceeds with personalisation and delivery

This design ensures consistent use of the same audience definition across multiple sends.

Example Use Cases

Planned Service Update - Use a maintained contact list of affected users to send a series of update messages over time.

Regulatory Notification - Send legally required communications to a fixed list of registered contacts.

Campaign Communications - Reuse the same contact list across multiple broadcasts to ensure consistency.

5.3 File Import for Bulk Sends

Overview

File Import for Bulk Sends enables organisations to send messages to large audiences defined outside the platform, using files such as spreadsheets or CSV exports. This feature is designed for situations where recipient data is supplied on a one-off or periodic basis and does not need to be permanently maintained as a contact list.

File import integrates fully with Broadcast's validation, personalisation, security and audit mechanisms, ensuring bulk communications remain accurate, compliant and traceable.

File imports can be used in two ways:

- **Temporary (ad-hoc) sends**
  The file defines the audience for a single broadcast. Imported data is used only for that execution and not retained as a reusable list.
- **List-building or augmentation**
  Imported data can be used to create or update a contact list for reuse in future broadcasts, subject to governance and permissions.

This flexibility supports both operational and strategic communications.

Supported File Types and Structure

Broadcast supports common, structured file formats suitable for bulk messaging, including:

- CSV (comma-separated values)
- Other delimited text formats where configured

Each file typically contains:

- One row per recipient
- A header row defining the fields (e.g. email address, phone number, reference identifiers)

Header Mapping and Field Configuration

When a file is uploaded, headers are mapped to known contact fields:

- Users or systems define how each column relates to a contact attribute
- Mandatory fields (e.g. delivery addresses) are validated
- Optional fields can be used for message personalisation tokens

This mapping ensures imported data aligns with the platform's contact model and prevents mismatches or missing data during sending.

Personalisation with Imported Data

Imported file data can be used directly for personalisation:

- Columns may be referenced by tokens in message templates
- Each recipient receives a tailored message based on their row's data
- Default or fallback values can be applied where configured

This allows highly personalised bulk messages without requiring pre-existing contact records.

Recipient Resolution and Deduplication

During send execution:

- Each row in the file is treated as a potential recipient
- Duplicates are detected and handled according to configured rules
- Imported recipients can be combined with contact lists or dynamic groups
- Explicit exclusions (contacts or groups) are applied

The final recipient set is always deduplicated before dispatch.

Example Use Cases

Operational Notifications - Upload a daily export of affected users to notify them of service issues.

Event Communications - Send reminders to attendees using a registration spreadsheet.

One-Off Regulatory Messages - Deliver mandated communications to a supplied list without creating a permanent contact list.

---

6 Auditability and Metadata

Auditability and Metadata provide end-to-end traceability for all Broadcast activity. Every broadcast, message variant and send execution is recorded with clear ownership, timestamps and status information. This enables organisations to demonstrate accountability, support compliance requirements and investigate issues confidently.

The service is designed to support environments where transparency, assurance and evidential records are essential.

6.1 What Is Recorded

Broadcast maintains structured metadata across the full lifecycle of a communication, including:

Broadcast definition data

- Unique identifier
- Client (tenant) ownership
- Creator or initiating user
- Descriptive labels and references
- Tags and categorisation

Change and usage history

- Creation date and time
- Last updated date and time
- Last used date
- Cloning relationships (provenance from earlier templates)

Message configuration

- Channels used (email, SMS, voice)
- Personalisation tokens referenced
- Short-link configuration
- Two-way handler configuration

Send-Time Audit Records

Each execution of a broadcast generates runtime records that capture:

- When the broadcast was triggered
- Whether it was manual, scheduled or project-driven
- The resolved audience size
- Per-recipient send attempts
- Delivery status per channel
- Errors or failures encountered

These records form a verifiable history of what was sent, when and to whom.

Delivery and Response Tracking

Audit records include:

- Delivery receipts from providers
- Timestamps for sent, delivered and failed states
- Inbound responses from recipients (where enabled)
- Handler outcomes for replies and status events

This allows organisations to demonstrate:

- Proof of sending
- Proof of delivery (where available)
- Evidence of response handling.

Appendix C – Functional Specification for API Messaging

1 Overview

The Boomerang Messaging Direct API enables businesses to send and manage email, SMS, voice, RCS, WhatsApp and two-way conversational messages through a single, secure REST interface. It supports bulk messaging, inbound replies, delivery receipts, short-link tracking, social-hours controls, and privacy-focused masked conversations. With flexible campaign tagging, scheduling, and real-time response handling, the API is designed for scalable, reliable customer communications and seamless integration into existing systems.

The API specification is set out in Swagger Hub and accessed via the following link:

https://app.swaggerhub.com/apis/BoomerangMessaging/boomerang-messaging_direct_api

Appendix D – Functional Specification for Microsoft Messaging

1 Overview

Boomerang Microsoft Messaging enables organisations to deliver intelligent, automated, and conversational messaging directly from Microsoft applications, extending communication capabilities without the need for bespoke development. The service integrates seamlessly with Microsoft's ecosystem, allowing messaging to be embedded within existing business processes and workflows.

1.1 Microsoft Custom Connector

Boomerang's Custom Connector exposes its omni-channel and Intelligent Messaging capabilities to Microsoft Power Automate, Power Apps, and Azure Logic Apps. This allows organisations to design and automate 1-way and 2-way broadcast messaging, as well as fully conversational stakeholder engagements, directly from Microsoft services. The connector supports integration with Dynamics 365 CRM and ERP, alongside other Microsoft-connected applications such as Azure services, IoT Central, and Microsoft Teams, enabling rapid deployment of messaging-enabled workflows within familiar tools.

The functional specification for Boomerang's Custom Connector can be accessed via https://learn.microsoft.com/en-us/connectors/boomappconnect/

1.2 Dynamics 365 Messaging Plug-In

The Dynamics 365 Messaging Plug-In provides native access to SMS messaging from any Dynamics 365 application. Unlike traditional SMS integrations that are limited to notifications, Boomerang's plug-in automatically matches outbound messages with incoming responses, recording all activity within the contact timeline. This enables true conversational engagement and allows responses to act as triggers for real-time automation within Dynamics workflows, supporting more responsive and efficient business processes.

The functional specification for Boomerang's Dynamics 365 Plug-In can be accessed via

https://boomlink.uk/d/s/tF6qRWvXDVtKOmrRUK6xHSA3rwWp6K7S/rX0iqLRq2smeu0_P0r2yMBsiFfYBj5UZ-bb3gzxi7Tws

Appendix E – Functional specification for Email-to-SMS and Email-to-Voice Messaging

1 Overview

A service that accepts email messages submitted from an email client to a designated Boomerang email address (that includes the recipient's mobile number). The email request is then converted to an SMS or voice message and sent to the number provided in the email address. 1-way and 2-way and conversational messaging are supported and where 2-way or conversational messaging are used, recipient responses are converted back to an email message and sent to the originating email address.

---

2 Access

The service is accessed from an email client by sending an email message to a designated email address provided by Boomerang. The service will only accept requests originating from an authorised email domain or series of authorised email addresses. It is also possible to restrict access to a mail server address. Spoofing is protected against by using SPF rules which ensure that the IP address used to send an email must match that set in the SPF record.

---

3 Communication Channels

The service supports global messaging over SMS and Voice (delivered as Text-to-Speech).

---

4 Messaging Solutions

The following messaging solutions are supported:

- 1-Way SMS Messaging – Messages are delivered to the recipient's device with an alpha originator which is set in the Email Subject field. The recipient is unable to reply
- 1-Way Voice Messaging – Messages are delivered via a telephone call with the message content played via text-to-speech
- Conversational messaging – Separate conversational threads are automatically created based on the Email Subject between the service user and the recipient this

---

5 Messaging features

The following features relating to outbound messaging are available:

- **Fixed originator (SMS) –** Use a static dynamic header as the originator for all outbound SMS messages. 2-way messaging is not supported where a fixed originator is used.
- **Message Disclaimer –** Pre-defined, custom content that is appended to all outbound SMS or voice messages.

- **Character Limit –** Messages containing more characters than a pre-defined threshold value set by the customer are not sent, and an error message is returned to the user.
- **Signature Manager** – A pre-defined, custom value that is used to denote the end of a message. Any content located after the specified value is not included in the message.
- **Delivery status notifications –** Provides the option to receive status updates for the messages for which a failed or undeliverable notification is returned by the recipient's network operator. Notifications are sent as an email to the originating user.
- **Social hours** – Provides the ability to set the times between which messages will be sent by Boomerang. Messages received by Boomerang between are only processed outside of the designated 'Social Hours'.
- **Secure Data** – Message content, response content and communication addresses are overwritten.

---

6 Service management

Access to Boomerang's user interface to manage service settings for:

- **Security** – Define system user access by adding individual email addresses (with the option to trigger a welcome email to new users), an email domain, an IP address or a mail server address.
- **User management –** Add and edit system users and control access through configurable user roles consisting of a structured permission set.
- **Outbound messaging** – configuration options relating to the attributes of an outbound message.
- **Service notifications** – Set Email and URL addresses to which unmatched responses can be forwarded.
- **Communication Defaults** - Configure default attributes for SMS and voice communications.

---

7 Reporting

7.1 Dashboard View

Summary reports are provided via widgets in a Dashboard view covering messaging activity, system activity and information relating to the status of your account.

7.2 Transaction Reporting

Reporting tool providing the ability to build customised reports relating to messaging activity and system activity including reporting by:

- Period / Date Range – Predefined selections or custom date range
- Transactions – Number of individual message transactions
- Billable – Number of billable records

- Communication channel
- Message direction (1-Way / 2-Way)
- Inbound messages and replies
- Message delivery status
- Individual recipients

Reporting data is accessed as either graphical chart or via a tabular view containing the detailed transactional message data relating to the parameters selected.

Appendix F – Specification for Inbound Communications

1 Service Overview

The Inbound Communication service receives, models, and processes inbound communications from external senders. These communications may arrive via SMS, email, or other supported channels and are automatically routed to configured handlers based on address, keywords, and client-defined rules. Inbound enables organisations to accept incoming messages, apply routing logic, trigger automated workflows, and capture auditable records for reporting and analytics.

---

2 What the Service Does

The Inbound service:

- Receives inbound messages from external systems or users.
- Normalises message data across supported channels (for example SMS or email).
- Matches inbound messages against configured handlers using deterministic rules.
- Routes matched messages to asynchronous processing workflows.
- Persists inbound message records and handler matches for reporting and audit.
- Provides searchable and filterable inbound message statistics via an API.

An inbound message may match zero, one, or multiple handlers depending on configuration.

---

3 Supported Channels

Inbound supports multiple communication channels, including but not limited to:

- SMS
- Email
- WhatsApp

Each inbound message is explicitly associated with a channel, and handlers are evaluated only against messages on the same channel.

---

4 Inbound Message Model

Each inbound message includes the following attributes:

Field	Description
Channel	The communication channel used (for example SMS number or Email address).
To	The destination address, phone number, or mailbox that received the message.

From	The sender's address or phone number.
Content	The body of the message.
Subject	Optional subject line (used for email-like channels).
Attachments	Optional list of files included with the message.

4.1 Attachments

Attachments are supported as optional components of inbound messages.

Each attachment includes:

- **Filename** – original file name.
- **Body** – base64-encoded file contents.
- **Content Type** – MIME type (for example **image/png**).

Attachments are typically supplied as structured JSON objects by integrations.

---

5 Handler Configuration and Matching

5.1 Handlers

Inbound messages are evaluated against configured handlers (also referred to as inbound rules).
Handlers are defined and managed by clients and determine:

- Which inbound addresses or patterns they apply to.
- Whether they act as exact matches or wildcards.
- Optional keyword requirements.
- Whether the handler is active or inactive.

Handlers are associated with a specific client and project.

---

6 Matching Logic

When an inbound message is received, the service applies the following matching steps:

1. **Channel filter**
   Only active handlers configured for the same channel are considered.

2. **Inbound address matching**
   A handler matches the inbound destination (**To**) using one of the following methods:

   - **Exact match**: the handler is not a wildcard, and the inbound address exactly equals the message destination.

- **Wildcard partial match**: the handler is marked as wildcard and its configured inbound value appears as a substring within the message destination.
- **Wildcard global match**: the handler is marked as wildcard and has no inbound value configured, allowing it to match any destination on that channel.

3. **Client status check**
   Handlers belonging to inactive clients are ignored.

4. **Keyword matching (optional)**

   - If a handler defines keywords, the message content must start with one of those keywords.
   - Keyword matching is case-sensitive and applied as a strict prefix check.
   - If no keywords are defined, the handler automatically passes this check.

All handlers that satisfy these conditions are considered matches. There is no limit to the number of handlers that may match a single inbound message.

6.1 Processing After Matching

For each matched handler:

- Metadata about the match (such as handler, client, and project) is logged.
- Usage counters are incremented for reporting and operational insight.
- Persistent records are created for:
  - The inbound message itself.
  - The handler match (hit), including timestamp information.

This design supports scalable processing and does not block inbound message receipt.

6.2 Inbound Handler Actions

When an inbound message matches an active handler, the handler can perform one or more predefined actions. Actions define **what happens next** once a message has been recognised and matched. Actions are executed asynchronously and do not block the receipt of inbound messages.

Automated Reply (Auto-Reply)

Handlers can be configured to send an automatic response back to the original sender of the inbound message.

Key characteristics:

- The reply is sent on the same channel as the inbound message (for example SMS replies to SMS, email replies to email).
- The destination of the reply is automatically derived from the inbound message's **From** address or number.
- The response content is defined by the handler configuration and may include:
  - Static text.
  - Predefined templates.

- Auto-replies can be used for acknowledgements, confirmations, help messages, or simple command responses.

Example use cases:

- Sending “Thank you, your request has been received.”
- Returning balance or status information in response to a keyword.
- Providing instructions when an unknown command is received.

Workflow Triggering

Handlers can initiate one or more automated workflows when an inbound message is matched. This allows inbound messages to:

- Start business processes.
- Integrate with downstream systems.
- Enrich or transform message data.
- Route messages to internal teams or systems.

The inbound message data (such as sender, content, subject, and attachments) is made available to the workflow for processing.

Forwarding / Routing

Handlers may route inbound messages to other destinations or systems, depending on configuration.

This can include:

- Forwarding message content to external Emails, APIs, or services.
- Passing inbound data to internal systems for further handling.
- Routing messages based on keywords, inbound address, or channel.

---

7 Reporting and Search

7.1 Inbound Statistics

The service provides reporting on inbound messages and handler matches. Supported features include:

Filters

- Client identifier.
- Date range (from and to).
- Free-text search across sender, destination, content, subject, handler labels, references, and descriptions.

Pagination

- Offset and limit-based pagination.
- Limit values are constrained to a defined maximum.

Ordering

- Results can be returned in ascending or descending chronological order.

Results

- A list of inbound messages with associated handler information.
- A total count of matching inbound messages.

This is represented via administrative dashboards, operational reporting, and audit review.

---

8 Common Use Cases

Dedicated inbound address - Route messages sent to a specific phone number or mailbox to a single workflow.

Shared address with keywords - Use keywords to distinguish commands or intents on a shared SMS short code or email inbox.

Fallback or catch-all routing - Use wildcard handlers to ensure all inbound messages on a channel are captured or responded to.

Domain or pattern matching - Apply wildcard matching for email domains or address patterns.

Appendix G – Functional Specification for Monitoring & Alerting Service

1 Overview

The Monitoring and alerting service provides automated monitoring and alerting for digital services, APIs, and external conditions. It enables organisations to define monitors that run on a schedule, evaluate results, and automatically trigger dedicated alerting and response workflows using Boomerang's workflow engine, provisioned within each customer's account.

By combining monitoring with configurable workflows, the service supports proactive detection of issues and consistent, automated communication and response processes.

---

2 What the service does

The Monitoring service continuously checks defined targets or conditions and records their status. When checks run, the service can trigger automated workflows by passing structured variables to other systems.

The Monitoring service:

- Executes checks against configured targets or conditions
- Maintains the current health status of each monitor
- Detects failures, recoveries, and state changes
- Triggers alerting and response workflows to manage communications and actions

Monitoring results are passed as structured inputs into workflows, allowing organisations to automate alerting, escalation, and operational responses.

Typical uses include:

- Monitoring website or API availability
- Validating response codes, timeouts, and content
- Supporting recovery workflows after failures
- Triggering alerts or automated actions based on external conditions (such as weather)

2.1 Monitor types

The service supports two main monitor types:

Ping monitors

Used to check URLs or API endpoints. These monitors perform regular "pings" to verify availability, performance, and response behaviour.

Weather monitors

Used to monitor weather conditions and raise alerts when configured thresholds or rules are met.

2.2 Key features

Scheduling and timing

- Monitors can be configured with optional **start** and **end** times.
- Checks only run while the monitor is active and within its configured time window.
- Each monitor can have one or more schedules defining:
  - Frequency (for example, every 5 minutes)
  - Days of the week
  - Time-of-day windows
  - Specific calendar dates can be excluded so checks are skipped when required.

Ping configuration

Each ping monitor includes at least one check configuration:

- **Liveness check** (mandatory): the primary health check that runs regularly.
- **Recovery check** (optional): used after a failure to confirm recovery under different conditions.

Checks can be configured with:

- Target URL, path, and port
- Timeouts
- HTTP headers
- Expected success response codes
- Optional response body matching rules

Weather configuration

The weather monitor uses official Met Office forecast and ensemble data to provide trusted, forward-looking weather intelligence rather than reactive observations. The monitor allows configurations for:

- **Flexible geographic targeting** - Alerts can be scoped country wide, by region, or by county, enabling monitoring aligned to operational footprints.
- **Multi-day forecast alerting** - Conditions can be evaluated for today up to six days ahead, supporting proactive planning and early warnings.
- **Time-of-day awareness** - Weather conditions can be assessed for daytime, nighttime, or both, enabling context-specific alerting.
- **Rich condition types** - Supports multiple forecast parameters including significant weather, wind speed, wind direction, gusts, visibility, temperature, humidity, and probability of snow.
- **Threshold-based rules** - Alerts trigger when forecast values equal, exceed, or meet defined thresholds, allowing precise control over alert sensitivity.
- **Multiple conditions per monitor** - Users can define and combine several weather conditions within a single monitor.
- **Colour-coded severity** - Conditions can be assigned visual severity indicators to support prioritisation and escalation.
- **Workflow-driven automation**
  When conditions are met, structured alerts trigger automated workflows for notifications, escalations, or operational actions.

2.3 Status and lifecycle

- Monitors have a lifecycle state: *draft*, *active*, or *archived*.
- Only active monitors run.
- The system maintains a status for each monitor, including:
    - Last check result
    - Current health state (for example OK or failing)
    - Next scheduled run time
- Next run times are automatically calculated based on the configured schedule.

2.4 Triggers and automation

When a monitor runs, it can dispatch triggers to other parts of the system or integrated services. Triggers include structured variables such as:

- Monitor name, description, and priority
- Current status
- URL checked
- HTTP response code and response body (where applicable)

Users can also define custom variables on a per-project basis to support integration with downstream workflows. Triggers are processed asynchronously to ensure monitoring checks remain responsive and scalable.

---

3 Alerting workflows and communication management

The service includes a range of configurable alerting workflows designed to manage communication and response processes when monitoring events occur. These workflows are built on Boomerang's workflow engine and are provisioned directly within the customer's account, ensuring customers retain control, visibility, and ownership of their alerting logic.

3.1 Workflow capabilities

Alerting workflows can be configured to:

- Send notifications to defined recipients or systems
- Escalate incidents based on severity or duration
- Route alerts to different teams depending on context
- Handle failure and recovery events differently
- Record audit and operational logs

Workflows can be tailored to organisational policies and operational requirements, supporting consistent and repeatable communication processes.

---

4 System Event Management

Events can be created automatically when Monitoring tools within the CPaaS platform raise alerts, as defined in more detail in Monitoring Triggered Events.

5 Security and data protection

- Sensitive configuration values, such as HTTP header values, are encrypted before being stored.
- Encrypted values are only decrypted at runtime when a check is executed.
- Free-text fields are sanitised to prevent injection or content-related issues.
- The service follows secure error handling and logging practices.

6 Data handling and persistence

6.1 Creation and updates

- Monitors are created and updated using operations to prevent duplication or conflicts.
- Related configuration (such as API connections) is managed transactionally to avoid partial or inconsistent data.
- Validation is performed on save to ensure required configuration is present and correctly formatted.

6.2 Deletion

- Deleting a monitor also removes its associated checks and related configurations in a single transaction.
- This ensures no orphaned or partial data remains.

6.3 Standards and formats

- Date and time values use RFC3339 format (for example: **2026-01-13T15:04:05Z**).
- Scheduling and execution align checks to consistent minute boundaries.

7 Service limitations

- Ping monitors must include exactly one liveness check.
- Only one recovery check is permitted per monitor.
- Monitoring runs only when the monitor is active and within its configured schedule.
- If required system variables are missing from a trigger configuration, monitoring will continue but a warning may be logged.

8 Service management and support

8.1 Monitoring visibility

Users can view:

- Monitor configuration

- Current and historical status
- Upcoming scheduled run times

---

9 Typical use cases

9.1 Automated incident alerting

- A service fails a health check
- Monitoring triggers an alerting workflow
- The workflow sends notifications and escalates if required

9.2 Recovery confirmation

- A recovery check passes
- A workflow records the recovery and updates stakeholders

9.3 Policy-driven communications

- Alerts are routed to teams based on severity and context
- Communication follows predefined organisational processes

Appendix H – Functional Specification for Logic Solutions

1 Overview

Solutions are pre-configured, custom communication and automation workflows and designed to fulfil specific business processes. Each Solution is purchased individually and delivered as a managed cloud service.

Solutions combine workflow logic, messaging channels, integrations, reporting, and user controls into a single, ready-to-use capability. They are configurable to customer requirements without the need for bespoke development and form part of the wider Boomerang platform service offering.

---

2 Solution Catalogue

The Solutions portfolio includes, but is not limited to:

- Lone Worker – Duty of Care
- Incident Communications
- Field Force Communications
- Customer Satisfaction Surveys (SMS / Web)
- Contact Centre Engagement
- Service Desk Ticketing
- Business Continuity Communications
- Machine-to-Machine (M2M) Alerting
- Service Outage Notifications (SLA Compliance)
- Appointment Rescheduling
- Resource Management – Workforce Fulfilment
- Shift Planning
- Automated Marketing Campaigns
- Information Requests / Booking Requests
- Debt Recovery
- Logistics – Delivery Management
- Mustering – Personnel Recall
- Instant Authentication (2FA)

Each Solution is delivered as a pre-built workflow that can be deployed via API integration and/or executed directly through the user interface.

---

3 Functional Capabilities

Solutions leverage Boomerang's CPaaS messaging and workflow platform capabilities, including:

- **Pre-built templates and configurability** – Solutions accessed as ready-to-use workflow templates that can be configured (content, timing, channels, rules) without bespoke development.

- **Workflow orchestration and automation** – Pre-configured, multi-step Logic workflows automate end-to-end business processes using triggers, timers, parallel actions, and conditional paths.
- **Multi-channel communications** – Send and receive two-way communications across SMS, Email, Voice, WhatsApp, RCS and web forms, with configurable retries and escalation paths.
- **Response capture and handling** – Capture structured replies (e.g. keyword or free text, form submissions) and store them decision-making, reporting, or onward processing.
- **API integration and interoperability** – Ingest requests from third-party systems and return outcomes or updates via APIs, enabling system-to-system automation such as appointment rescheduling or service desk updates.
- **Conditional logic and decisioning** – Apply rules and branching logic based on user responses, timeouts, thresholds, or external system data to dynamically control workflow behaviour.
- **Data capture and variable management** – Store, update, merge, and transform data within workflows using variable actions to maintain state across short or long-running processes.
- **Escalation and exception handling** – Automatically escalate non-responses, critical alerts, or failures to alternative users, channels, or teams, with error handling and recovery options.
- **Reporting and operational visibility** – Provide real-time status, delivery metrics, response tracking, and outcome reporting via the user interface to support SLA and operational monitoring.
- **Auditability and governance** – Maintain audit trails of workflow execution, actions, and decisions, with role-based access controls and governed configuration to support compliance requirements.

Solutions are used to accelerate deployment and reduce implementation time, with full customisation as required.

---

4 Delivery Models

Solutions are delivered using one or both of the following models:

4.1 API-Integrated Solutions

Solutions can integrate with third-party applications such as CRMs, booking systems, service management tools, or line-of-business platforms using secure APIs.

Typical flow example:

- A third-party system sends a request containing recipient and contextual data (e.g. appointment details).
- The Solution workflow manages outbound communications, reminders, retries, and channel selection.
- End users respond using defined options (e.g. confirm, decline, reschedule).
- Boomerang processes responses and returns outcomes to the originating system.
- Where required, the Solution performs look-ups or follow-up interactions (e.g. presenting alternative appointment slots).

This model supports fully automated, system-to-system workflows with minimal user intervention.

4.2 User Interface-Driven Solutions

Solutions can also be executed directly via the platform user interface without API integration. For example:

- Mustering or personnel recall scenarios
- Incident or business continuity communications
- Ad-hoc engagement or survey execution

In these cases, authorised users trigger pre-defined workflows through the UI, with all responses, status updates, and reports available within the platform dashboards.

---

5 Workflow Configuration and Governance

Solutions are built on governed workflow components and actions, including messaging, data extraction, API calls, and AI-enabled steps where applicable.

Controls include:

- Central libraries for approved workflows and templates
- Version control and audit logging
- Role-based permissions for configuration and execution
- Customer-specific policies for content, data handling, and access controls.

---

6 Channels and Communications

Solutions support multi-channel communications, including:

- SMS
- Email
- Voice
- WhatsApp
- RCS
- Web links and forms

Channel selection, escalation, and fallback behaviour are configurable per Solution to ensure reliability and response optimisation.

---

7 Reporting and Insights

Each Solution includes reporting and dashboards that provide visibility into:

- Delivery success rates
- Response and engagement metrics
- Workflow performance and outcomes
- SLA and compliance-related indicators

These insights support operational monitoring, service improvement, and audit requirements.

---

8 Commercial Model

- Solutions are purchased individually under transparent pricing models.
- Pricing reflects the configured workflow, channels used, usage volumes, and service tier.
- All pricing is published and compliant with G-Cloud 15 requirements.

---

9 Suitability for G-Cloud Customers

Solutions are suitable for:

- Central government departments
- Local authorities
- NHS and healthcare bodies
- Emergency services
- Arms-length bodies and public sector agencies

They are designed to support operational communications, service delivery, resilience, and citizen engagement use cases.

Appendix I – Specification for AI Services

1 Overview

The service includes an AI and Large Language Model (LLM)–enabled platform that allows customers to create, configure, and use AI-driven capabilities through a secure user interface, email integrations, and application programming interfaces (APIs). The AI capabilities are designed to support operational efficiency, decision-making, and information management while maintaining strong governance, transparency, and compliance controls.

---

2 Purpose of AI Processing

The purpose of AI within the service is to assist users in analysing, transforming, and generating information from documents, messages, and structured or unstructured data. AI is used to automate routine tasks, surface insights, and support workflows, helping organisations reduce manual effort and improve consistency and accuracy.

---

3 Scope of AI Capabilities

AI capabilities provided by the service include, but are not limited to:

- Document and data processing, including summarisation, comparison, extraction, classification, and content creation
- Automation of workflows and decision support tasks
- Natural-language interaction through UI, email, and API interfaces
- Aggregation and analysis of information across multiple documents or datasets
  These capabilities can be embedded into existing workflows and systems as part of the wider service offering.

---

4 AI Functional Capabilities

The service's AI functionality supports:

- Ingestion of multiple data and document types via UI, email, and APIs
- Interpretation and understanding of document structure and content
- Generation of summaries, structured outputs, and draft responses
- Comparison of documents and identification of changes or inconsistencies
- Extraction and structuring of key data fields
- Classification, redaction, and anonymisation of content
- Insight generation, including trends, sentiment, and risk indicators
  AI tasks may be executed individually or combined into end-to-end automated workflows.

---

5 Service Interfaces

AI capabilities are accessible through:

- A secure web-based user interface
- Email integration for submitting and receiving AI-processed content
- APIs (where enabled), allowing integration with customer systems
  AI may also be embedded directly into other service features, such as message composition or content quality checks.

---

6 Governance, Controls, and Safety

The service includes governance mechanisms to ensure AI is used safely, responsibly, and in line with organisational and regulatory requirements. These include:

- Role-based access controls and feature permissions
- Restrictions based on document type and data sensitivity
- Query and output safety controls to prevent inappropriate or unauthorised use
- Logging and audit trails of AI activity
- Approval workflows for higher-risk AI processes
  These controls support transparency, accountability, and risk management.

---

7 Data Handling and Compliance

AI processing operates within defined data governance rules, including:

- Configurable data retention and deletion policies
- Controls for anonymisation, redaction, and masking of sensitive data
- Clear separation of customer data based on service model
- Support for compliance with data protection, privacy, and information security requirements
  These measures help ensure lawful, proportionate, and secure AI usage.

---

8 Account and Service Models

The service supports different account models to balance cost, control, and capability, including shared and exclusive AI service options. These models define data isolation, access rights, and availability of integration features such as APIs.

---

9 Reporting and Transparency

Customers and administrators have access to reporting and dashboards that provide visibility into:

- AI usage, consumption, and allowances
- Workflow execution and performance

- Operational health and system status
- Compliance-related activity and audit information
  These reports support operational oversight, billing transparency, and governance.

---

10 Summary

The AI component of the service is designed to deliver practical, governed, and transparent AI capabilities suitable for public sector use. AI is applied to clearly defined tasks, operates within robust control frameworks, and supports compliance, accountability, and value for money in line with G-Cloud principles.
