Service Definition - G Cloud 15

Alert Cascade

Critical Communication Suite

Contents

About Us 3

Solution Suite Overview 4

Core Platform Access (CPA) 7

Optional Extras 9

Data and Security 10

Training, Support, and Maintenance 14

Service Levels 19

About us.

We specialise in providing highly resilience emergency and mass notification services – Alert Cascade are one of the only truly UK based providers, with our staff physically located here in the UK and available to assist you 24/7/365. Our current cloud-based solutions have been built from scratch, and we own them 100%, giving us the ability to pivot quickly if your needs change, work with you to provide a solution that works specifically for your needs and your local demographic, and keep pace with technology and infrastructure changes.

We've worked with some of our clients for over 15 years. During that time, sector specific hazards, the general threat horizon, and the regulatory environment, have all changed considerably – and our solutions have changed and grown alongside our customers. Whilst many of our customer relationships are subject to Non-Disclosure Agreements (NDAs), we're proud to highlight some of the organisations we already work with here in the UK:

- NHS Bath, North East Somerset, Swindon and Wiltshire Integrated Care Board
- Energy Networks Association (ENA)
- University Hospitals of Northamptonshire
- City of London Polic (CoLP)
- Royal Wolverhampton NHS Trust
- Hinkley Point C Nuclear New Build
- Sellafield Limited
- Humber Emergency Planning Service
- University of Cambridge
- Swindon Borough Council
- Cumberland Council
- South Yorkshire Local Resilience Forum

Solution Suite Overview

24/7/365 access and management

Alert Cascade's critical communications suite is a modular Software as a Service (SaaS) messaging platform, built on a secure, scalable, and reliable infrastructure with multiple layers of redundancy to enable rapid delivery of critical communications. Our solutions are permission based, so you can control who can send alerts, create message templates, access contact data stored within your service, and manage your account settings.

Although our UK-based support team is available 24/7/365, we understand that customers need to be self-sufficient in accessing and managing their Alert Cascade service. You can use Alert Cascade on any internet enabled device (desktop, tablet, smartphone, etc.) without the need to install a dedicated app. Because of this, provided you have Wi-Fi, 5g, or 4g available, you will be able to send an alert. If you don't have internet access available, authorised users can trigger alerts via a phone call to your dedicated alerting line, by SMS text to your alerting inbox, or by email to your alerting distribution list.

We deliberately designed our platform to guide users though critical tasks, and to provide self-service tools to manage your users effectively without having to raise a support ticket:

- Password reset (for yourself, or for another lower-level user).
- Re-issue welcome emails and 2FA set up instructions.
- Unlock users locked out due to repeated failed login attempts.
- Promote and demote users.
- Temporarily prevents contacts from receiving alerts.
- Temporarily disable users from logging in to the dashboard.
- Tag users to automatically receive copies of all message reports.
- Create and manage distribution lists to receive system notifications.
- On screen filters to show users with no phone number or empty data fields.

Data gathering

The most important aspect of effective messaging is the quality of information you have stored in your service. To help with this, customers use a simple 2 step process to create unlimited custom fields to store contact data and any other relevant information you need to group your contacts or make your message reports more meaningful.

Rather than enforce a rigid set of fields that may not work for you, we help you create a set of custom fields that exactly match the information your have available in your data source(s). Setting up your account this way reduces training needs (because we-re re-using field names you already have in other systems) and makes sure your Alert Cascade service is working around your needs (because the only fields that exist are the ones you've identified as needed).

Customers use a variety of different methods to maintain their data:

- Manually via the secure web dashboard
- Imported via the dashboard using a .csv file
- Automatically imported via our inbuilt SFTP connector
- Updated in real time via API
- Collected via a bespoke Registration Portal
- Contact self-sign up via web portal, dedicated SMS inbox, or QR code

Whichever data maintenance method you use, our flexible data maintenance wizards automatically reformat phone numbers to the correct format (regardless of spaces, brackets, hyphens, etc.) and check they are valid "in use" numbers, as well as deduplicating and validating email addresses. Because our wizards handle the formatting and validation automatically, you don't need to spend time cross-checking and amending your source data – you can present it in raw format.

Multi-channel outbound communications

Our core messaging channels include voice calls, SMS text, and email alerts. Additional channels are available, and include push notifications, Microsoft Teams integration, Slack integrations, and Conference Bridge. Your account will be delivered with the core notification channels and any additional channels agreed in the contract. Additional channels can also be added at any point during the contract by mutual written agreement. All channels are 2 way enabled and will collect real time replies, enabling you to make evidence-based decisions – use cases include mobilising staff, confirming safety, and gathering feedback on the effect of any IT outages.

Messaging in Alert Cascade revolves around the **Message Form** – we use a single area to create and manage message templates, send template or ad-hoc messages, and pre-schedule messages on a one off or recurring basis. The benefit of this is that from a training perspective, new users only have to focus on learning a single tabbed layout and because of this, they can be up and running very quickly.

Dynamic distribution groups for sending your message are created automatically based on the information you have chosen to store within Alert Cascade e.g. if you have stored office locations for your contacts, there is automatically a distribution group created for each location. You can also create manual distribution groups if you need to pick and choose individuals rather than rely on their location, skills, or other attributes. There are no limits to the number of fields you can create in Alert Cascade, or the amount of data you can store for each individual contact, so there are no limits on the number of distribution groups you can create within your service.

Real time reporting shows delivery statuses per individual and aggregated number and % of responses received, what responses were received, from whom, by what device and channel, and when. Live report graphs show snapshot summaries, whilst the detailed reports drill down to individuals, allow you to combine criteria (i.e. show me everyone on the gold team who hasn't replied), and export via .csv, .xlsx, and PDF (permission dependent).

Core Platform Access (CPA)

Resilient automated messaging

All Alert Cascade services include the following features as standard:

- 2-way voice, email, and SMS communication channels.
- Dedicated domestic phone number for use with all outbound calls, branded SMS sender name, dedicated SMS sender numbers, and fixed email sender addresses.
- Unlimited message templates with option to pre-schedule on a one-off or recurring basis.
- Advanced polling (set up to 10 response options on a per message basis).
- Advanced sending rules (use multiple sending criteria i.e. send to staff in location X, with a skill set of Y's, and a role of Z).
- Quick Send (use the same content for all channels) and Advanced Send (use different content for each channel).
- SMS and email attachment support.
- Self-service web application dashboard available on any internet enabled device.
- Ability to trigger alerts via SMS text, email, or voice call in addition to via secure web dashboard.
- Real time reports with live graphical views and detailed "drill down" options.
- Unlimited customisable device and data fields for storing information about contacts.
- Ability to mark fields as Personally Identifiable Information, enabling easy compliance with GDPR/DPA, and helping with DPIA.
- Data maintenance directly via the dashboard, manual file import, automated SFTP import, and API.
- Permission based access allowing you to segregate data processing and message sending roles.
- Unlimited concurrent administrator access to the services.
- UK/EU secure hosting for all aspects of your account, including support.
- Set up – work with a dedicated Implementation Specialist via screenshare, including setting up configuration and default preferences, initial data upload, and sending your first alert.
- Ongoing support – UK based support team, available 24/7/365.

Service Definitions

Contacts	Message recipients, who receive and reply to your alerts. You can allow Contacts to log in and directly manage their own data if you wish, but no other service access is available.
Users	People who can log in to the service and carry out either data maintenance, account management, or message sending activities.
Single Agency Account (SAA)	Subscription plan for customers who need to send alerts to their own staff (or relatives/associates of those staff). For example, NHS Trusts, British Embassies, University Hospitals.
Multi Agency Account (MAA)	Subscription plan for customers who need to send alerts to their own staff and multiple external organisations. For example, Local Resilience Forums (LRFs), Integrated Care Boards (ICBs), local authority emergency planning teams.
Local Authority Account (LAA)	Subscription plan for local authority customers who need to send business continuity alerts, operational notifications, and IT outage notifications, either to all staff or to key segments.
Education Account (EA)	Subscription plan for education sector customers who need to send alerts to staff, faculty, students, and/or parents.
Primary Agency	The lead agency in an MAA, who has procured the services. For example, for LRFs, this will be the host organisation.
Recipient Agency	An agency in an MAA whose staff are Contacts that receive alerts from the Primary Agency. Recipient Agencies can have their own Users, however, they are limited to data maintenance of their own Contacts.
Sender Agency	An agency in an MAA who have their own Users who can carry out data maintenance of their own Contacts and send alerts to their own Contacts. Some Contacts in a Sender Agency will receive alerts from the Primary Agency, some will receive alerts from the Sender Agency, and some will receive both.

Optional Extras

Additional modules available to complement CPA

Document vault(s)	Secure document vault, with option to attach files to email and SMS messages.
Workflow automation	Automated workflow rules with incident logging, management, and trend analysis.
Information hotline(s)	Inbound information hotline, with unlimited inbound capacity. Standalone, or integrated with CPA.
Conference bridge	Call your team and "bridge" them into the conference when they answer.
Mobile push notifications	Additional notification channel allowing Contacts to receive alerts on their mobile phone via a downloadable Progressive Web Application.
MS Teams integration	Additional notification channel allowing Users to send alerts to Teams Channels*, or to individual Contacts** via chat.
Slack integration	Additional notification channel allowing Users to send alerts to Slack Channels*** via chat.
Desktop alerting	Additional notification channel allowing Contacts to receive alerts on their desktop via a downloadable Progressive Web Application.
Smart Assistants	Ability to trigger alerts using Smart Assistants (Amazon Echo, Google Assistant, and Apple Siri).
Registration portal(s)	Branded secure web portal allowing Contacts to sign up to receive alerts. Optional SMS text, and QR code sign up routes available with this module at no extra cost.
On Call	Shift, schedule, and calendar-based alerts. Create schedules from scratch, import existing rotas, or allow Contacts to manage their own availability.

* Customer will need access to create webhooks in their MS Teams instance.

** Customer will need to provide API access to their MS Teams instance via the Microsoft Graph API.

*** Customer will need access to create webhooks in their Slack instance.

Data and Security

Security, compliance, and audit

As a critical communication provider, we process data (including personal and sensitive data) daily, making information and cyber security a top priority. Our hosting environment is accredited to ISO9001, ISO27001, ISO27017, ISO27018, SOC1/SSAE 16/ISAE and PCI DSS Level 1. As a business, we hold Cyber Essentials Plus, ISO27001, and ISO9001, we're registered with the ICO as Data Controllers in our own right, and we're governed by Ofcom. We have an EU and Swiss representative in line with our obligations under the GDPR, and we hold "Standards Exceeded" rating in the NHS Data Security and Protection Toolkit.

We routinely carry out application scanning and third-party penetration testing, and our customers are encouraged to do the same. We run application scans in line with OWASP on all development and staging environments, the results of which require documented Information Security (IS) team sign off prior to deployment in the production environment.

Customer data is encrypted at rest and in storage. We do not transfer data to an offsite location since all 3 server locations operate in mirror image hot standby mode. Enforced TLS is required for email communications with customers. Cryptographic controls including SSL and TLS 1.2 are used at the web interface. Data is encrypted using dual layered AES-256 i.e. at both the physical hardware level and the database level.

Access to all Alert Cascade modules is permission based, and every screen and feature adheres to the "Privacy by Design and Default" protocol. This allows customers to provide access to key staff on a limited access basis so that they can trigger alerts, without providing access to the personal data that's stored in the account.

Our staff can only access customer data within the designated data processing environment. This environment can only be accessed via the fixed Ips in the support areas using 2FA devices which are located within the support

environment, allowing data exchange when necessary to fulfil our contractual support obligations, but not allowing anything outside of that. Alert Cascade staff will not access customer data via laptops or mobile devices. Removeable media are not available within the support environment i.e., no USB drives, no laptops, tablets, or mobile devices.

Data transfer mechanisms are fully documented – we do not support physical media as a data transfer method and operate a paperless office environment in all locations. Appropriate data protection controls are in place in line with ISO27001, the EU GDPR, the UK DPA, and all relevant data protection legislation to the locations our customers are based in.

Customer records are stored within the AWS EU and UK data centres and will be retained for the lifecycle of the contractual arrangements in place between the Customer and Alert Cascade. Our application does not create backups due to the triple redundancy hot standby model; changes to Personal Data are enacted in real time.

Because we're Data Controllers ourselves, all staff are fully conversant with your (and our) obligations, so you'll find plenty of helpful tools within our solutions. One of the most important tools is the ability to flag fields in your account as containing personally identifiable information. Using this flag lets us categorise those fields differently, and make sure that if a contact is removed from your account, their personal data is fully removed form your database, and from any reports you have created.

As Alert Cascade is a self-service platform, we also have a responsibility to help users make sensible choices about their own security:

- **Audit tool**: allow Users to check their own activity to make sure they recognise it and allow Admins to audit whole account activity.
- **Password suitability checker**: checks new passwords against a list of 10,000 common or "bad" passwords, and against a list of over 100,000 passwords that have been breached in other places.
- **User log in checks**: monthly emails to system administrators highlighting users who have not logged in for 3 or more months. Users would normally be

expected to log in at least quarterly, even if only to check that they are still able to log in – Users who don't log in regularly should be reviewed to make sure they really need that level of access.

- **Lock out alerts**: if a User is locked out for security reasons, all administrators are notified in real time so they can assess whether this is expected behaviour.
- **Bespoke security policies**: set account policies for how many logins and password reset attempts a user is allowed, how long users should be locked out for, and password complexity rules.

Audit logs capture administrative activity, all User activity (including login and authentication attempts, whether successful or not), and system faults. The audit logs include the data and time stamp, information about the event, which user or system action was involved, and which processes were involved. Logs are stored in a location that is protected against tampering and unauthorised access and are available in a read only format to users with Admin level permission.

Logs are searchable, filterable, and exportable in the dashboard, providing an easy route to GDPR and DPA compliance with regards to traceability and transparency of data processing activities. In addition, some actions (such as data downloads and data imports) can be configured to send automatic email notifications to customer admins.

When required, our support team can provide forensic level logs to law enforcement agencies or customer security teams to aid with incident investigation.

Performance, reliability, and scalability

The core function of Alert Cascade is to allow customers to send critical alerts. Therefore, resource allocation within the application will always give priority to message sending functions. We also auto scale resources within customer accounts as needed and can scale resources manually if we become aware of the potential for traffic peaks before customers start sending messages.

The application runs in mirror image hot standby across 3 geographically disparate areas within the EEA, and our own support staff are geographically disparate within the UK to ensure full coverage 24/7/365 regardless of any localised incidents. Our failover capabilities for DR/BC revolve around using either our secondary or tertiary server locations, effectively providing an RPO and RTO or zero due to the hot standby. We use the same process to make deployments to the production environment, to ensure there is no disruption to customers during deployments. This means that we use our failover process in a live situation approximately twice per month, in addition to the full tabletop exercises conducted as part of our own BC, DR, and Operational Resilience processes.

Bearing in mind that our application is a tool designed to be used by customers when they're experiencing a business disruption of their own, our architecture is specifically designed to remove single points of failure – we use multiple data centres, multiple telephony and email carriers, and multiple monitoring systems that sit outside of the AWS architecture.

We have a risk-based Business Continuity and Disaster Recovery (BC/DR) program in place, compliant with ISO22301, which includes the following:

- Documented and approved BC/DR policy.
- Procedures to supplement the requirements laid out in the BC/DR policy.
- A process to review the goal and objectives of the BC/DR program on an ongoing basis.
- A formal review of the BC/DR program and plan on an at least annual basis, or whenever there are significant changes to processes/technologies supporting our operations.
- Our plans consider our response to a potential cyber-attack, and the full program is reviewed and approved by senior management at least annually.

Training, support, and maintenance

24/7 support with ongoing training

Alert Cascade is deliberately designed to require a low level of training – our secure web dashboards are icon and Q&A led, with detailed tips available on every screen. Each part of the solution suite is designed with the knowledge that our services won't be used daily so must be simple enough to use in an emergency with little to no training.

All accounts include access to our online help and support centre; this includes a series of "quick start" video guides centred around the core needs of importing data, sending messages, and interpreting message outcomes via your reports. The quick start section is designed for new starters to your organisation and can also be used as refresher training for staff who have Alert Cascade access but haven't had the need and/or opportunity to use the service recently.

The FAQ section covers what we hear most often during our onboarding sessions – we update this area monthly so that we can capture topical questions and share them with all our customers. Our help and support centre includes over 100 more detailed articles that walk you through each screen of your service, explain the different options available, and provide guidance on not just how to do something, but why we recommend doing things a certain way.

Our support ticketing process includes the option for you to book a training webinar with one of our account specialists on a subject of your choice. Training sessions are recorded in a downloadable format so that you can easily share them with colleagues.

When we add new features to Alert Cascade, release notes are issued automatically to anyone who currently has dashboard access – where appropriate, release notes will also include links to new training videos centred on the new feature.

Much of Alert Cascade is self-service – Users can reset their own password, customer Admins receive automatic notification if a User is locked out and can unlock them, and proactive monitoring takes place to inform you of Contacts who don't have any phone numbers so would be difficult to reach during an emergency, or Users who haven't logged in for a long time so may struggle to do so in an emergency.

However, during an incident, the speed of message sending and delivery is critical. Because of this, you can opt for our support team to hold standing authority to launch alerts on your behalf. Subject to being able to identify you on the phone, our teams will take your detailed instructions and send the communications for you. Once they've sent the messages, they will work with you to resolve whatever issues stopped you sending the alert in the first place.

Implementation planning and onboarding.

During initial onboarding, we create a bespoke training plan based on the specific needs of the individual customer and their use case. The initial priority is to ensure that core Users can send an alert from day 1, and the training plan then moves on to more detailed subjects including:

- Creating message templates relevant to the specific risks the customers are addressing with their business continuity, operational resilience, and major incident plans.
- Best practice for message sending – how to share information using Plain English standards, message length, when to use different channels, when and how to include links to further information.
- How to interpret reports and use past results to improve your messaging.
- Conducting regular tests and tabletop exercises – setting test objectives, monitoring response times against KPIs, incorporating Alert Cascade in your ISO27001 and ISO22301 objectives, when to involve us.
- Trouble shooting common data issues and improving your data maintenance process.

Typical implementation timescales are under 2 weeks – many customers are up and running within 48 hours, and we can deliver same day accounts if required. A typical implementation plan includes:

- **Implementation kick off**: Initial orientation call – our support team liaises with you to identify who will be involved in the implementation, any specific time constraints (annual leave, industrial action, etc.) and agree timescales for follow up steps. During this call, we will discuss what we need from the customer in terms of successful implementation, introduce the Alert Cascade team, and confirm the support contact information. This is usually a 30-minute call on day 1.
- **Customer preparation**: Identify Champions and other roles who will be involved in the implementation, identify data sources for contact/other data, and review any existing BCPs or emergency arrangements so it's clear internally where Alert Cascade will fit into your existing processes.
- **Initial delivery**: We will deliver your Alert Cascade service with all contracted features enabled, ready for customisation to meet your specific needs during

training (adding your own fields, branding, etc.). Using the data source you've identified, our support team will carry out your initial import. Phone numbers and emails will be reformatted and validated during import, so you do not need to "clean" your source data first.

- **Training**: We carry out our training via webinar at times to suit the Champions, and sessions are recorded so they can be shared internally as needed. The initial training focusses on the core features to get you up and running as soon as possible, with follow-up sessions for advanced features if needed. Access to your help and support (including videos) is available from day 1, and typically customers can use the core service elements with a single 1-hour training session.
- **Follow up and project close**: Once your training has been delivered, our support team will check in with the Champions to make sure they have everything they need. During the initial delivery and training phases, we encourage customers to send test messages to themselves and others and gather feedback from message recipients. We provide examples of "best practice" during training, and during follow up will help you tweak your configuration based on recipient feedback.

To achieve a successful implementation, it's important that the right people are involved during onboarding:

Role	**Responsibilities**
Alert Cascade (AC) project manager	• Main point of contact, co-ordinates the AC resources. • Agrees the scope, deliverables, and timescales. • Communicates progress updates. • Dedicated for the duration of the project.
AC support team	• Provides initial and follow-up training to the customer champions. • Gathers feedback on training to ensure it is effective. • Provides support on recommended AC configurations based on customer use case. • Provides support on data maintenance best practices and carries out the initial import. • Dedicated for the duration of the project.
AC specialist team	• Manages the SaaS platform and provides detailed technical support for specialist use cases.

AC account manager	• Liaises with the customer to make sure their needs are being met. • Dedicated for the duration of the project.
Customer contract owner	• Main point of contact, co-ordinates the customer resources.
Customer champions	• Individuals nominated by the customer – this team should include an HR representative, and IT representative, and at least 1 end user of the service. To send messages effectively, you need to be able to rely on your data. Customer champions must have access to the source systems that will be used to import into Alert Cascade.

On-site training and implementation is available by request at an additional cost; most customers prefer remote implementation as this allows for greater flexibility for their attendees and requires less customer resources overall.

Service levels

99.999% guaranteed uptime

Our SLA is 99.999% availability, defined as the percentage of total time during which the services are available without critical issues. The following 5 levels of criticality apply:

- **Change request**: Changes to configuration that cannot be made through the secure web dashboard by a customer User. Outside of the scope of the SLA
- **Self-serve**: Assistance with configuration alterations where those changes can be made via the secure web dashboard by a customer User, or general questions about how to use the services. Time to respond 72 hours.
- **Minor**: Non service affecting issues, including but not limited to problems with reports and intermittent delays on the secure web dashboard. Time to respond 12 hours, time to fix 24 hours.
- **Serious**: Issues which result in delays and/or intermittent failures including but not limited to delays in alerts being sent, and the secure web dashboard being unavailable for all customer Users. Time to respond 6 hours, time to fix 12 hours.
- **Critical**: Service affecting issues which result in total failure to transmit outbound communications. Time to respond 30 minutes, time to fix 3 hours.

SLA remedy:

Description	**% of monthly subscription fee credited**
Failure to achieve availability SLA	100
Failure to achieve resolution time - Critical	100
Failure to achieve resolution time - Serious	75
Failure to achieve resolution time - Minor	50
Failure to achieve resolution time – Self-serve	25