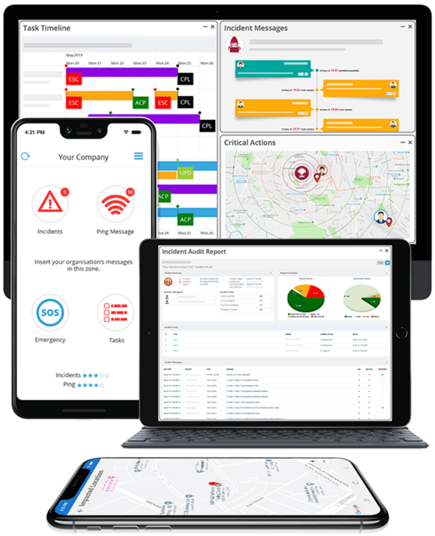

CRISES CONTROL

G-Cloud 12 Framework Service Description Document

Most Innovative Mass Notification
& Security Platform - 2020
Corporate Excellence
Awards 2020

Unified
Communications
Product of the Year

Cloud DR and
Continuity Product
of the Year

ISO
22301
Business
Continuity
Management

Enabler

UK Office:
19 Heather Park Drive, Wembley
HA0 1SS

www.crises-control.com
+44(0) 208 584 1585

Confidentiality

Crises Control submits this Service Description based on the information supplied at the time of its drafting. This is a Confidential document and contains Crises Control confidential and proprietary information, specifically for evaluation by the addressee company on the understanding that it is not to be disclosed to any third party without the express permission of Crises Control. This document remains the property of Crises Control at all times and no part thereof may be reproduced or transmitted in any form or by any means, without prior written approval from Crises Control. Use of any copyright notice does not imply unrestricted public access to any part of this document and all trademarks are acknowledged as the property of their rightful owners.

Contents

Contents

Introduction

Company Overview

Organisations face a variety of challenges, ranging from the overall landscape of today's internal and external information security threats to potentially dangerous and emergency situations that could arise on or around operating locations. As a result, there is increasing pressure on management to provide faster, more insightful and more transparent communications during crises. With critical, dangerous and emergency situations becoming more likely, more frequent and wide-ranging in impact, organisations need a secure and reliable way to communicate with all stakeholders.

Crises Control ensures that all organisations (including SMBs, Enterprises, government authorities and healthcare organisations) are prepared to respond to unexpected events within the critical event life cycle, speeding communications and response to mitigate the impact of a critical event. The Crises Control platform provides a state-of-the-art two-way communication service designed to ensure efficient, reliable and documented responses and coordination across a variety of platforms. From text to voicemail to smartphones, alerts are transmitted instantly to each recipient on multiple devices, increasing the likelihood of quick responses. Crises Control's efficient and reliable service will provide customer with all the tools needs to effectively manage any crisis at all stages.

Features allow recipients to respond to alerts or complete a surveying / polling response. Recipients can select one of up to fifty response (if required) options specified by the alert sender. The service automatically collects responses sent by email, SMS, phone and mobile push and desktop alert. Crises Control treats all re-broadcast alerts as a new single alert for traceability. Additional Crisis Communication and Collaboration tools like one touch conferencing, event monitoring, task management and real time geo location alerting are available as part of the service.

Overview of the G-Cloud Service

The Crises Control Platform offers a number of modules which can support your organisation from daily routine communication to emergency situations:

1. Ping, a mass notification engine designed to send short messages to any distribution list within your Crises Control community.
    a. Public Alerting is a Ping Extension. It allows you to easily upload contacts and send them a 1-way message with no requirement for acknowledgements.
2. Incident Manager, an incident management platform designed to support your organisation in preparing predefined templates, launching and managing the alert at a later date.
    a. Task Manager and Checklists are Incident Manager extensions. They enable you to create to distribute tasks/ checklists to your users in a timely, effective and controllable way.
    b. SOS Facility is an Incent Manager extension. This gives your users a Panic / emergency / SOS button which allows them to notify you of an emergency situation.

Data and Maintenance

Data Processing and Privacy

Customer retains all ownership of the provided data to be included in the Send Word Now solution. Crises Control is fully GDPR compliant.

Where Crises Control is the Processors of your data, Crises Control ensures that this data is processed lawfully, fairly and transparently as agreed by our clients and to maintain appropriate security controls. Processing includes maintaining the confidentiality, availability, integrity and security of the data, the servers and network where the data is held. If it exceptionally necessary to access a client database to investigate a client issue, Crises Control will always seek the client's permission in advance. Crises Control prides itself on its premium security standards. In particular:

- We encrypt many of our services using SSL. Our SSL rating is A+.
- We offer two factor authentication (2FA) verification when you access your Crises Control Account.
- We use Cloudflare Advance Security to protect and secure the application and APIs against denial-of-service attacks, customer data compromise, and abusive bots.
- We have Data Protection Addendum (DPA), which is a contractual agreement in place with Cloudflare to protect our customer's data to EU- GDPR standards.
- We encrypt data whilst at rest.
- We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorised access to systems.
- We restrict access to personal information to Crises Control employees, contractors and agents who need to know that information in order to process it for us and who are subject to strict contractual confidentiality obligations. They may be disciplined, or their contract terminated if they fail to meet these obligations.
- We are ISO27001, ISO9001 certified.
- We employ certified GDPR practitioners to maintain and improve security standards.

Cloud Hosting Arrangements

Crises Control is hosted using UKCloud (https://ukcloud.com/). UKCloud are providers of a services cloud for the exclusive use of UK Public Sector organisations. UKCloud Enterprise Compute Cloud provides our customers with the trusted, connected and flexible Assured OFFICIAL cloud platform you need to deliver your critical enterprise applications in the cloud. The platform can help you achieve the business goals at the center of your strategy, without risking your operational ability to execute.

- UK-based telephone service desk and Network Operations Centre (NOC), providing 24/7 support for P1 critical incidents and proactive monitoring, including access to UKCloud's technical experts

- Platform optimised for OFFICIAL SENSITIVE data and fully aligned to the National Cyber Security Centre (NCSC) 14 Cloud Security Principles
- Extensive independent validation by recognised UK public sector authorities, which enhances the platform's suitability for especially sensitive workloads for organisations within the health, police and defence communities
- Multiple secure UK data centers separated by more than 100km and connected by high-bandwidth, low-latency dedicated connectivity
- UK sovereignty — assured cloud platform delivered by a UK-based company with UK government security-cleared personnel
- Platform hosting workloads exclusively for the UK public sector, creating a known and trusted community of neighbours
- Option of connection to public sector networks including:
  - Public Services Network (PSN Assured)
  - New NHS Network (N3/HSCN)
  - Joint Academic Network (Janet)

Backups, Restoration & Disaster Recovery

Crises Control guarantees 99.95% uptime and availability as part of our robust Service Level Agreement (SLA). Our geographically-distributed data centers are completely active-active for immediate failover with no delay in recovery time. Data and processing logs are continuously backed up from the primary node to the secondary via a high-speed VPN connection. In the unlikely event of primary node failure, the secondary backup node assumes responsibility for the continued provision of service.

Crises Control's Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) are reviewed and tested on twice a year.

Solution Maintenance

As a SaaS model, all Crises Control customers run on the same version of the software. We deploy approximately one release per month as required by maintenance and security updates. Major releases, with functionality changes, new features, etc. are deployed alongside the maintenance and security changes on a monthly basis. Software releases do not result in customer downtime, nor do they impact the availability of the service for customer use. Our Service Level Agreement guarantees 99.95% uptime and availability.

Using the Service

Onboarding

The highlights of our standard project plan are as follows. The Implementation Projects are customized per individual account based on specific client requirements. Your Crises Control Support Manager and/or Project Manager will coordinate the implementation offering guidance and best practices until you sign off the implementation program.

The provision of the following services constitutes the scope:

- Welcome email/ letter
- Kick-off meeting
- Full assistance with account configuration, setup and onboarding of users
- Configuration of any Integrations or Automations
- Customisation and Confirmation meeting
- Full User training
- Account configuration call (including scenarios and associated components, such as notification modes, cascade defaults, from address, etc.)
- Provision of service manuals, platform walkthroughs and video tutorials
- Resolution of user issues, incidents and enquiries via the 24/7 Crises Control Service Desk

1.2 Service Levels

The Services delivered by Crises Control shall be delivered, managed and measured against a set of best practices deemed applicable to these Services. The Service adheres to the following quality standards/ recommendations:

- ISO9001:2008
- ITIL
- ISO 27001
- Cyber essentials

Your Customer Success Manager will, at all times, work to meet or exceed the Service Level Agreement in place. A dedicated Customer Success Manager (CSM) is assigned to every new account. The CSM will coordinate the implementation, training and remain a technical contact point for the duration of the contract.

Service Availability targets are the planned percentage of time for which the Service is in operation, excluding any planned maintenance downtime. The hosting platform is assured by Service Credits at 99.95% Availability.

1.3 Support and Service Levels

Severity	Criteria	SLA	Target Achievement
1	A fault exists that results in a total loss of service or functionality affecting a whole site (sites), or whole system or services	**15 minutes** to respond. **4 hours** to resolve.	100% of all Severity 1 Incidents will be resolved within the SLA
2	A fault exists which results in partial loss of service or functionality affecting multiple users	**1 hour** to respond. **8 hours** to resolve.	100% of all Severity 2 Incidents will be resolved within the SLA
3	A fault exists which results in loss of service or functionality for a single user	**1 hour** to respond. **24 hours** to resolve.	100% of all Severity 3 Incidents will be resolved within the SLA

The response time is the elapsed time from when the call is logged to when a defined service level response is made.

Resolution means that a permanent course of action or outcome of the reported issue has been agreed and the issue resolved.

Provision of the Service

Customer Responsibilities

The customer shall be responsible for:

- Ensuring that the data contained within the platform is appropriate and in line with corporate and information assurance policies
- Ensuring that there is some connectivity from the end-user's device to the Crises Control service

Ordering and Invoicing Process

Signed Service Order and T&Cs are required Service is invoiced annually in advance/30-day payment terms

Technical Requirements

To operate fully, the Service requires:

- IE8 (or equivalent Microsoft Edge, Chrome, Firefox or Safari) browser or later - accessed via a desktop/laptop
- Android, iOS or Windows Phone mobile device for the Crises Control App
- Internet/Telephony Network connectivity from the End-User's device

Contact Details

Crises Control
19 Heather Park Drive
Wembley
United Kingdom
HA0 1SS
+44 (0) 208 584 1385

Vittoria, Sales Director UK & Europe +44 (0) 7944 590 135

Vittoria.Nicastro@crises-control.com

www.crises-control.com