



Crown
Commercial
Service



Commercial
Services Group

G-Cloud 15

Lot 2b - Cloud Software

EmploymentCheck✓.

EmploymentCheck Online Right to Work (RtW) Platform

Service Definition Document

Cantium Business Solutions Limited.
(T/A Employment Check)

1 Abbey Wood Road, Kings Hill, West Malling ME19 YT
t: 0300 1249 996 e:bids@hrconnect.org.uk

Company No. 11242115 VAT No. GB294540288

Commercial Services Group is a trading brand for Cantium Business Solutions Limited (Reg No. 11242115) – a private limited company wholly owned by Kent County Council.

Contents

Introduction	3
EmploymentCheck Online Right to Work (RtW) Platform	3
Features and Benefits.....	4
About Us	4
Service Management	5
SLA, Including Support Hours and Availability	5
Service Desk Availability	6
Service Constraints	6
Training and Support / Consultancy	6
Financial Recompense for not meeting Service Levels	6
Onboarding and Offboarding	6
Onboarding	6
Implementation Plan	7
Offboarding	9
Outcomes and Deliverables.....	10
Trial Availability	10
Responsibilities and Requirements	10
Customer Responsibilities.....	10
Technical Requirements	10
Prices, Invoicing and Contracts	11
Pricing Model.....	11
Ordering and Invoicing.....	11
Contract Termination	11
Security and Resilience	11
Data Backup, Data Restoration and Disaster Recovery.....	11
Business Continuity and Disaster Recovery	11
Business Continuity and Disaster Recovery Objectives	12
Information Security.....	12
Our Organisational Controls	13
Security Management	13
Data Protection.....	14
Accreditations.....	14

Introduction

EmploymentCheck Online Right to Work (RtW) Platform

Our Right to Work (RtW) platform is a quick and easy way to carry out RtW checks through our online solution, EmploymentCheck.

All employers have a legal obligation to conduct Right to Work checks prior to employees commencing their roles. Experience the future of recruitment compliance with the Right to Work Check solution from EmploymentCheck. Streamline your processes, reduce errors, and ensure a hassle-free experience for both your team and applicants.

Designed to simplify and accelerate the verification of an individual's eligibility to work in the UK, Right to Work Check offers a comprehensive, UK government certified experience.

We are partnered with Yoti, the market leading Digital Verification Service (DVS) to offer a state-of-the-art integration for conducting electronic RtW checks. Use of the module speeds up the processing of pre-employment checks and ensures employees can be confirmed in post quicker compared to verifications completed manually.

Through our fully compliant, online, RtW checking solution, we:

- Offer three compliant routes for establishing the statutory excuse for an individuals' Right to Work in the UK.
- Leverage the market leading digital verification technology offered by Yoti Ltd via our integrated solution.
- Provide a reliable RtW service to organisations across the spectrum of public, private, health, and charitable sectors.
- Speed up the recruitment of individuals and reduce the admin burden involved in manual verification of applicant identity.

Features and Benefits

Features	Benefits
- Secure integration with a market leading Digital Verification Service (DVS) provider - Yoti. - Accessible anytime, anywhere, on any internet-enabled device. - Fully accredited UKDIATF provider. - Intelligent auto-validation ensures accurate data submissions. - Flexible email suite with reminders and notifications. - Comprehensive reporting suite with dashboards and analytics. - Full Role Based Access Control (RBAC) covering a range of user roles and permissions. - Multi Factor Authentication (MFA) solution available.	- Error-free applications through smart validation technology. - Expert support offered by dedicated internal team members. - Fast results via an efficient online platform. - Smartphone and tablet accessible for mobile convenience. - Continuous improvements from internal development teams. - Simple transactional billing with transparent pricing.

About Us

As a Local Authority owned trading organisation (LATCo) and wholly owned by Kent County Council, Cantium Business Solutions Limited has over 35 years' experience supplying IT services to the Public sector. As such, we have developed a comprehensive managed service portfolio, built alongside a strong partner network, to support and complement the services we deliver in-house.

We are in the privileged position of being part of a collection of brands under the Commercial Services Group with a joint focus on improving services within the Public Sector, from legal and procurement services to education advice, supplies and energy procurement.

Our highly experienced and dedicated teams consist of over 300 ICT specialists, who support over 33,000 service users across 700 organisations with expert advice and guidance.

As a Local Authority owned business, we are in the unique position to truly

understand the Local Government landscape. We appreciate the budget restraints faced within the Public Sector and the delicate balance between implementing new technologies and innovations, whilst ensuring the vital public services remain robust and unaffected by change.

- The Public Sector is part of our DNA
- Wholly owned by Kent County Council with our profits staying in the public sector.
- Successfully traded for over 35 years both as part of the Local Authority and as a standalone company.
- Experienced at delivering back-office services to a diverse range of customers.
- Commercially astute with a collaborative, partnership-based ethos and approach.
- ICT and Professional partner to over 700 organisations including local authorities, central government, NHS trusts, Multi-Academy Trusts and colleges.

Customer experience is at the heart of what drives us as a business, which has been solidified in our recent glowing report from our Customer Service Excellence (CSE) accreditation.

Service Management

SLA, Including Support Hours and Availability

We deliver a standard support service to the following SLAs:

Priority	Response Target	Resolution Target	Description
P1	2 Business Hours	10 Business Hours	Complete loss of service. Resolution target relates to RPO (Recovery Point Objective).
P2	5 Business Hours	20 Business Hours	An issue that results in a degradation/loss of service affecting over 50% of users. Resolution target relates to RPO (Recovery Point Objective).
P3	10 Business Hours	10 Business Days	A minor issue that results in a degradation/loss of service functions affecting more than one user but less 50% of users.

For service requests, the standard response times are as follows:

Response Target	Resolution Target	Description
5 Business Days	10 Business Days	Service requests such as bespoke reporting or ad hoc requests.

Service Desk Availability

Helpdesk Support	Availability
Telephone Support	08:30 to 17:30 (UK time), Monday to Friday excluding English Bank Holidays
Email Support	08:30 to 17:30 (UK time), Monday to Friday excluding English Bank Holidays

Service Constraints

There are no constraints applicable to this service.

Training and Support / Consultancy

Any training necessary for the deployment of this solution can be discussed with our onboarding team as part of your ongoing support and consultancy service.

Our team of DBS experts provide extensive training via webinars, as well as providing an in-depth system manual and links to pre-recorded system tutorials. We will provide supportive and constructive consultancy throughout the lifetime of your solution.

Financial Recompense for not meeting Service Levels

Please refer to our terms and conditions of sale for financial recourse arising from default by either party. Service credits are not included in this framework offer, unless defined within the service or product Service Level Agreement (SLA).

Onboarding and Offboarding

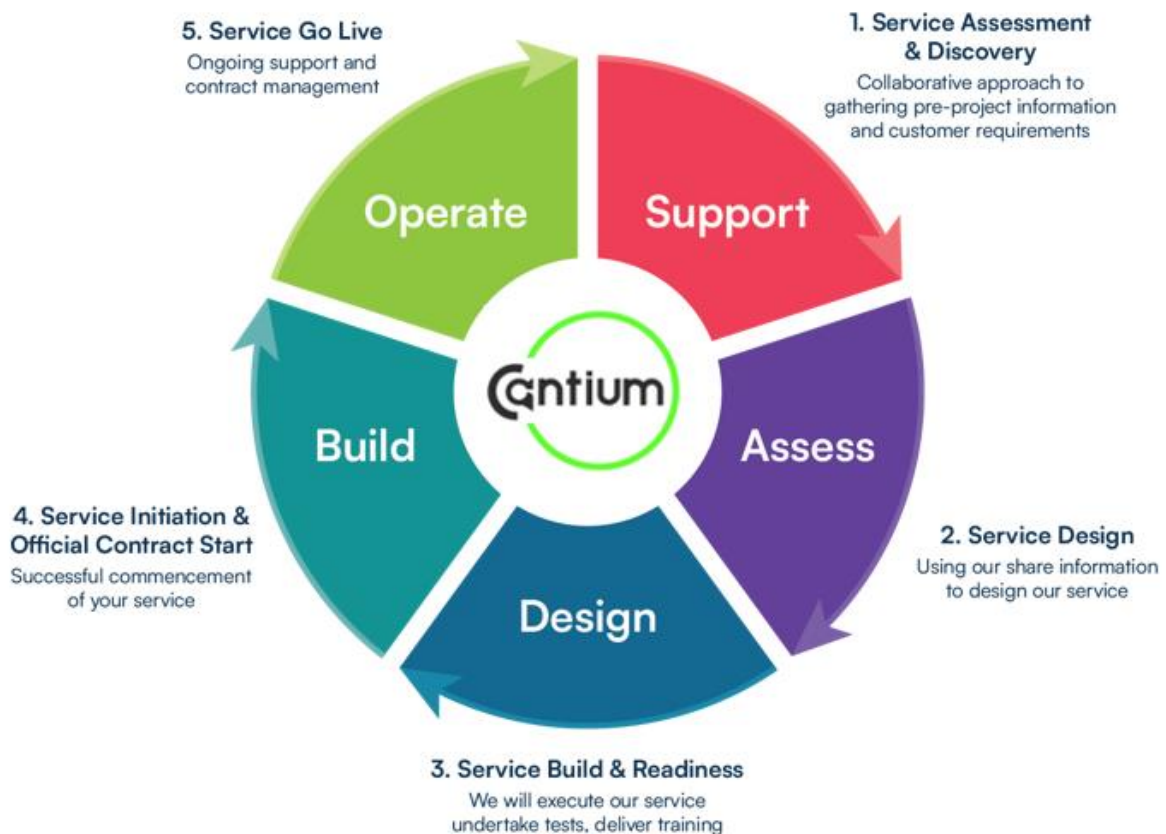
Onboarding

We prioritise establishing a clear and effective onboarding strategy with every new customer. We will ensure that every migration to a new application, software, or service is performed with the least possible disruption and highest possible satisfaction.

We make every effort to be as transparent as possible during the onboarding process.



Onboarding is our first opportunity to establish a great relationship with our customers; put simply, we know that first impressions matter. Our onboarding approach covers five key steps, as shown below:



Implementation Plan

From day 1, we will work with you in order to respect your needs and requirements.

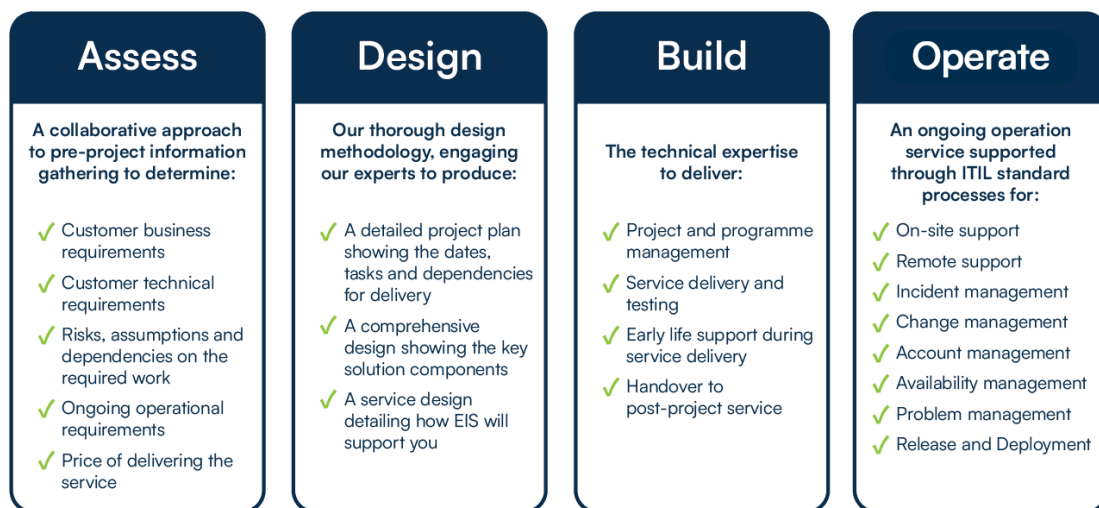
We will work together to outline your aims, create an implementation plan, and establish stakeholders in order to keep the Onboarding process as transparent as possible.

Our experience and expertise combine to create a truly bespoke service for your organisation. Using industry-leading, proven methods, we can work hand-in-hand with you to take your ICT Services to the next level.

We will work with you to create a bespoke support plan that caters to your organisation's individual needs. Your configuration set will be delivered in line with your priorities as part of the overall project scope.

Your Implementation Plan will follow the principles of our Project Delivery Approach. Every service, software, application, and consultancy that we offer follows these principles, ensuring your solution is planned and executed thoroughly.

Our delivery approach covers four key principles: Assess, Design, Build and Operate. A summary of these principles is as follows:



We take a collaborative approach to implementation, working together to incorporate your needs and requirements to create an implementation plan. To maintain transparency throughout the process, we will work together to outline your aims, create an implementation plan and establish key stakeholders.

Your implementation plan will follow the principles of our project delivery approach. Every service, software, application, and consultancy that we offer follows these principles, ensuring your solution is planned and executed thoroughly.

Your tailored implementation plan will be agreed upon with your onboarding officer during the onboarding process. Customers will receive a clear outline of how the solution will be implemented, including all required actions and assigning roles and responsibilities.

Customer Access Allows:

The following services are provided:

Provision of an online solution for conducting Right to Work checks. The solution supports three methods for completing Right to Work checks in line with Home Office guidance:

1) Using a Digital Verification Service (DVS) provider to undertake an online verification to digitally verify applicant documents which can be used to establish a statutory excuse.

EmploymentCheck is partnered with a market-leading, certified third-party DVS – Yoti. This integration enables digital verification checks to be undertaken for the purpose of completing Right to Work checks. The passport images and face scan images used for the digital verification check are returned to the EmploymentCheck system where they can be downloaded and stored locally.

The customer needs to retain this evidence for the duration of employment + 2 years.

2) Through a check of the applicant's Right to Work status online via the Home Office Share Code route. The 'Profile' page can be uploaded to the EmploymentCheck system, and an expiry date entered if required. This document can be downloaded and stored locally. The customer needs to retain this evidence for the duration of employment + 2 years.

3) By performing a manual check of the applicant's original documents. The copies of the original documentation can be uploaded to the EmploymentCheck solution, and an expiry date entered if required. These documents can be downloaded and stored locally. The customer needs to retain this evidence for the duration of employment + 2 years.

All three methods will provide an employer with a Statutory Excuse.

The Right to Work evidence and if applicable, the face scan image will only be stored on the EmploymentCheck system for 6 months after the Right to Work check has entered the 'Application Archived' status. After which point, the document evidence and face scan will be permanently purged from the EmploymentCheck solution.

Offboarding

We take offboarding and exit planning seriously, ensuring that our transparency and flexibility at the end of your solution's lifetime matches the beginning.

When offboarding, all property, data and information held in connection with the Framework or Call Off Contract will either be returned or destroyed as per our 'Secure Disposal Policy'.

An exit plan specific to your service requirements will be agreed as part of the onboarding process ensuring that you receive a bespoke service, and will be issued as part of the call-off

contract.

A typical exit plan for our EmploymentCheck DBS E-Broker Solution is as follows:

- Agree cut-off date with customer for submitting Right to Work checks.
- Remove the ability to submit new Right to Work checks after the agreed date.
- Grant view only access for an agreed period to meet data retention requirements. All non-essential users accounts would have their access to the system revoked.
- Archiving of application data and pass data to customer if required.
- All data destroyed after retention period specified in contract.

For details relating to Contract Termination, please refer to our G-Cloud framework terms and conditions of sale for rights to terminate.

All Offboarding process and Exit Plans must be agreed with in line with our Terms and Conditions of Sale.

Outcomes and Deliverables

Specific outcomes and deliverables will be agreed upon with your Onboarding Officer as part of the initial Implementation Plan. Part of communicating our shared vision is establishing clear outcomes and deliverables, working towards them, and reviewing them as part of our ongoing transparency.

Trial Availability

There is no trial available for this service.

Responsibilities and Requirements

Customer Responsibilities

All responsibilities between EmploymentCheck and the customer will be agreed upon before the Implementation Plan is executed. These responsibilities will be agreed upon in an SLA.

Technical Requirements

There are no specific technical requirements for this service.

Prices, Invoicing and Contracts

Pricing Model

Please refer to our G-Cloud rate card.

Implementation of the DBS platform may be subject to a set-up fee, dependant on the complexity of the customer's requirements. Any such charges will be levied in accordance with the published rate card.

Ordering and Invoicing

Customers will be required to complete and sign the G-Cloud framework offer terms and conditions order form.

All customers will be required to apply for a trade account and provide supporting evidence relating to all financial due diligence enquiries requested by EmploymentCheck.

Trade account payment terms are 30 days from issue date of an undisputed invoice.

While this is our standard approach, we aim is to make partnering with us as simple as possible. If you would like to discuss further options, please contact us at info@hrconnect.org.uk or telephone 0330 124 9996.

Contract Termination

For details relating to Contract Termination, please refer to the G-Cloud framework terms and conditions of sale for rights to terminate.

Security and Resilience

Data Backup, Data Restoration and Disaster Recovery

Protecting our customer's data is of paramount importance to us across all our services and sectors. Responsibility and openness when providing backup and restore services lies at the heart of every partnership we share with our customers.

Business Continuity and Disaster Recovery

Our approach to Business Continuity Management is aligned with industry best practice and standards including ISO 22301:2019. It provides a framework for corporate and service level management of business continuity to ensure that we remain resilient and able to continue to deliver services and recover effectively from

any significant business disruptions.

Our Business Continuity and Disaster Recovery (BCDR) plan details the processes and arrangements we (and our subcontractors) will follow to:

- Ensure continuity of our customers' business processes and operations supported by the services following any failure or disruption of any element of the deliverables; and
- Recover the deliverables in the event of a disaster.

Our BCDR plan is tested regularly to ensure its effectiveness in the event of a failure or disruption to the services.

Business Continuity and Disaster Recovery Objectives

Our Business Continuity and Disaster Recovery plan supports the delivery of the following objectives:

- To ensure continuity of provision of the deliverables in accordance with the Contract at all times during and after invocation of the BCDR plan.
- To minimise, as far as reasonably possible, the adverse impact of any disaster.
- To provide a process for the management of disaster recovery testing.
- To ensure compliance with security standards is maintained for any period during which the plan is invoked.
- To ensure BCDR arrangements are upgradeable and sufficiently flexible to support changes to the deliverables and business operations supported by them.
- To recover to standard operation mode with minimal disruption to services.
- To ensure lessons are learned and inform the continuous improvement of BCDR arrangements.

We undertake due diligence on subcontractors to ensure adequate BCDR arrangements are in place before engaging them as part of our supply chain and review this on an ongoing basis.

Where elements of the services are supported by any subcontractors, we and the subcontractor will each notify the other party in the event their respective BCDR plans are invoked. We will work together with the subcontractor to manage any failure or disruption in line with the BCDR arrangements in our contract with the subcontractor.

Information Security

We commit to ensuring that all personal and sensitive data processed on behalf of our customers is done so in accordance with Data Protection legislation, information governance and security best practice.

Our Organisational Controls

We will maintain appropriate organisational and technical measures to ensure the services we provide are secure and fully compliant with Data Protection legislation. These include, but are not limited to, the following:

- Data Protection, Information Security, Information Governance and related policies and procedures are in place and reviewed regularly. Copies of these can be provided upon request.
- All staff are required to complete mandatory Information Governance, GDPR/ Data Protection and Cyber Security e-learning which is renewed every two years.
- Physical access controls including swipe card/ ID card access to buildings, buildings opened and locked by security each day, clear desk and screen policy and control of access to secure areas.
- All staff contracts of employment include a clause detailing the responsibilities required of every individual when handling data of any kind.

Security Management

It is our policy to maintain an Information Security Management System designed to meet the requirements of ISO 27001. We have a dedicated Strategy & Governance team that is responsible for ensuring our organisation complies with all legal requirements, codes of practice and requirements prescribed to maintain our certifications which include ISO 9001, ISO 14001, ISO 27001 and Cyber Essentials Plus.

We have a range of established policies and processes to support the controls mentioned above, meaning you can feel safe in the knowledge that we have the necessary controls already in place to deliver a fully secure and compliant service. These include, but are not limited to:

- Statement of Applicability for Security Measures
- Acceptable Use Policy
- Access Control Policy
- Cyber Security Incident Management Policy
- Disposal and Destruction Policy
- Information Security Policy
- Password Policy
- Safe Use of Removable and Online Storage
- Software Update and Patch Management Policy
- Supplier Security Policy.

Data Protection

We are committed to fulfilling our obligations under the UK Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR) and the Data (Use and Access) Act 2025 and any subsequent data protection legislation, incorporating any appropriate additional obligations as required by the customer.

We are registered with the Information Commissioners Office (ICO) and have appointed a Data Protection Officer to monitor compliance with data protection legislation across our business activities.

Accreditations

