CareCheck

G-Cloud 15 (RM1557.15) Care Check Ltd

Provision of Disclosure and Barring Service Checks Service Definition Document

January 2026

1 Introduction 4
1.1 Document structure 4
1.2 How to use this document 4
Service description 5
2.1 About our service 5
2.4 Delivery framework 5
2.5 Service features / benefits 6
2.6 Service scope 6
2.6.1 Add-ons or extensions 6
2.6.2 Cloud deployment model 7
2.6.3 Service constraints 7
2.6.4 System requirements 7
2.7 Reselling 8
2.8 User support 8
2.8.1 Support details 8
2.8.2 Accessibility and usability 8
2.9 How users work with our service 9
2.9.1 Browsers 9
2.9.2 Desktop application 10
2.9.3 Mobile 10
2.9.4 Service interface 10
2.9.5 API 10
2.9.6 Accessibility and useability 10
2.9.7 Customisation 11
2.9.8 Service levels and availability 11
3. G-Cloud alignment information 13
3.1 Section introduction 13
3.2 Onboarding and offboarding processes 13
3.2.1 Onboarding 13
3.2.2 Offboarding 13
3.3 Data 14
3.3.1 Data importing and exporting 14
3.3.2 Analytics 14
3.3.3 Independence of resource 15
3.3.4 Public sector networks 15
3.3.5 Data-in-transit protection 15
3.3.6 Asset protection 15
3.4 Availability and resilience 15
3.4.1 Guaranteed availability 15
3.5 Governance 16

3.6 Security Governance **16**
3.6.1 Operational security 16
3.6.2 Staff security 17
3.6.3 Secure development 17
3.6.4 Identify and authentication 17
3.7 Auditing **18**
3.7.1 Performance monitoring and metrics 18
3.7.2 Compliance and quality management 18
3.8 Backup, restore & disaster recovery **18**
3.9 Training **19**
3.10 Service pricing **21**
3.11 Invoicing process **21**
3.12 Termination **21**
4.Security and data governance **23**
4.1 Data protection and encryption **23**
4.2 Data at rest, storage locations and physical security **23**
4.3 Data sanitisation and disposal **23**
4.4 Security testing and assurance **23**
4.5 Incident and protective monitoring management **24**
4.6 Configuration and change management **24**
4.7 Information security management and certifications **24**
4.8 Secure development and cryptography **25**
4.9 Identity and access management **25**
5. Supplier information **26**
5.1 About us **26**
5.2 Relevant experience and testimonials **27**
5.3 How to buy **27**

1 INTRODUCTION

1.1 DOCUMENT STRUCTURE

The Service Definition outlines the Provision of Disclosure and Barring Service (DBS) checks offered by Care Check under the G-Cloud 15 Framework. This document is divided into 3 core sections:

1. **Service description:** Presents an overview of the platform, including key features, benefits, user interface and support, accessibility, API capabilities and integration with HR/ recruitment systems
2. **Operational delivery and framework alignment:** Describes how our services are delivered, in line with the requirements of the G-Cloud 15 framework. This includes onboarding/offboarding, resilience, availability, data protection, security governance and incident management
3. **Supplier information:** Summarises our organisation, including our mission, credentials and experience, including guidance for buyers on how to procure our services on G-Cloud

1.2 HOW TO USE THIS DOCUMENT

This Service Definition is designed to support public sector buyers throughout the full G-Cloud procurement lifecycle. This includes early service evaluation through to contract award, delivery and ongoing service management. This includes:

- **Initial evaluation:** Section 2 (Service description) explains service scope, methodology and core benefits
- **Due diligence and contract planning:** Section 3 (G-Cloud alignment information) details onboarding, support arrangements, service levels, availability, resilience, data management and API capabilities
- **Data protection, security and resilience:** Section 4 (Security and data governance) describes information security framework and alignment with Cyber Essentials Plus principles, data handling standards and business continuity measures
- **Supplier assurance/verification:** Section 5 (Supplier information) details background information on Care Check, accreditations and guidance on how to procure its service through G-Cloud 15 framework

2. SERVICE DESCRIPTION

2.1 ABOUT OUR SERVICE

Care Check is a leading Disclosure and Barring Service (DBS) service provider. With **23** years' experience, we work across healthcare, education, recruitment, charity, financial construction, transport, defence, police and social care sectors, supporting organisations of all sizes in delivering faster recruitment decisions. Ensuring the highest standards of security, compliance and resilience for public and private sector organisations, we are **Cyber Essential Plus** accredited and the system which we use is **ISO27001** certified. Under the G-Cloud 15 framework, Care Check provides a secure cloud-based platform for conducting basic, standard and enhanced DBS checks as well as associated services such as:

- Digital ID verification
- Right to Work checks
- Social media checks

Reducing administrative burdens and accelerating recruitment decisions, our platform integrates with our customer's HR, recruitment and onboarding systems via API. Improving workflow efficiency, the platform complements existing software such as applicant tracking systems, payroll platforms and employee management tools. Evidencing its benefits, the platform is designed to address common recruitment challenges, including:

- Delays and inefficiencies in applicant verification
- Risk of non-compliance with safeguarding and employment legislation
- Administrative burden from manual tracking and paperwork
- Inconsistent data management across HR and onboarding systems

Acting as a trusted delivery partner, our approach is distinguished by:

- On average more than 25% cheaper on DBS admin fees
- More than 60% cheaper for Right to Work and ID Checks
- No registration fee
- No charge for API

2.4 DELIVERY FRAMEWORK

Ensuring consistent, secure and compliant service delivery, Care Check operates a structured platform lifecycle that is designed around the full customer journey. In line with DBS Codes of Practice, we follow:

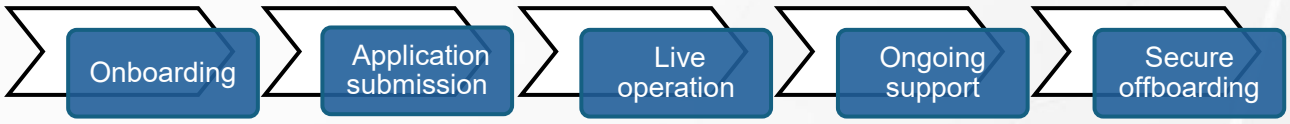


Figure 2.2.1: **Our delivery framework**

2.5 SERVICE FEATURES / BENEFITS

Feature	Benefit
Online DBS checks completed securely	Removing delays from paper-based processes and ensuring compliance with safeguarding/employment requirements, our platform enables employers to securely complete basic, standard and enhanced DBS checks online. This results in faster recruitment decisions with full adherence to legal standards.
Digital ID verification	Eliminating the need for in-person verification and streamlining onboarding, Care Check enables digital ID verification through mobile NFC passport scanning and live selfie uploads. The outcome is a secure, efficient identity check that improves applicant experience.
Right to Work validation	Ensuring employers meet statutory obligations before hiring, the system validates UK Right to Work eligibility using passport details or Home Office share codes. The outcome is reduced delays and a full audit trail for compliance purposes.
Social media screening with clear traffic-light risk assessment reports	Supporting employers in making informed decisions, the platform assesses public social media content and generates easy-to-read traffic-light reports. By highlighting potential risks, the outcome is safer recruitment with consistent oversight of potential safeguarding or reputational issues.
Role-based controls aligned to organisational permissions	Ensuring sensitive data is protected, the platform provides configurable access controls, restricting users to only the information relevant to their role. Maintaining GDPR compliance, this results in enhanced data security and controlled information sharing across teams.
Real-time DBS progress tracking through live dashboards	Supporting transparency, Employers can monitor the status of all checks in real-time through intuitive dashboards within the platform. Improving operational efficiency and minimising recruitment bottlenecks, this enables Employers to anticipate delays
Integrate systems via API	Enabling secure data exchange with customer systems and reducing duplications, Care Check integrates with HR, recruitment and onboarding systems through secure APIs, free of charge. This results in faster processing, reduced administrative effort and improved information accuracy

Figure 2.5.1: Benefits and features

2.6 SERVICE SCOPE

2.6.1 Add-ons or extensions

Providing flexibility for our customers, the platform can operate as an add-on or extension to other software services, while also fully functional as a standalone platform. Enabling automated submission and tracking of DBS, ID, Right to Work and social media checks, our service connects with customer HR, recruitment and onboarding systems via API. Improving workflow efficiency and reducing manual administrative tasks, it works alongside existing software such as Applicant Tracking Systems (ATS), payroll platforms and employee management tools. Any integration with an ATS must be initiated and developed

by the ATS provider using our API. All integrations are supported through secure, standards-based communication.

2.6.2 Cloud deployment model

We deliver our service primarily as a Public Cloud solution, hosted within secure UK-based data centres operated in line with recognised industry security and data-protection standards. To support disaster recovery and business continuity, application and database servers are located in 2 separate UK data centres. The architecture supports scalable, multi-tenant deployments and can be adapted for dedicated or hybrid environments where required by the buyer. Enabling buyers to meet local governance or interoperability requirements, where hybrid deployment is selected, we host core components in the cloud while integration points or data-processing elements can be deployed on-premise.

2.6.3 Service constraints

The constraints of our platform are limited to:

- Support is available Monday to Friday, **09:00-17:00** UK time, excluding public holidays and is not provided outside these hours
- Planned maintenance may result in temporary service unavailability, but buyers are given at least 48 hours' advance notice wherever possible
- Full application data is retained for 6 months, after which certain elements, such as the DBS result and snapshot report, are removed and the remaining data is archived in line with DBS Codes of Practice. If an application is withdrawn, most data is cleansed immediately, leaving only minimal basic information. All archived application data is fully removed from the system after 6 years
- Digital ID and Right to Work checks require compatible mobile devices with NFC and camera functionality enabled, which may limit use on older or unsupported devices. Applicants must use Android devices running at least Android 5.0 or Apple devices running at least iOS 7. Both front and rear cameras must be available and the Firefox browser may be unsuitable for this process
- Once applications have been submitted to the DBS, they cannot be amended and may be subject to delays caused by external DBS or police audits, which are outside our direct control

2.6.4 System requirements

To ensure optimal performance, the platform requires the following minimum system configuration:

- **Supported browsers:** Latest versions of Chrome, Edge, and Safari are recommended. Firefox is not advised for digital ID verification processes
- **Operating systems:** Windows 10+, macOS 12+, Android 5.0 or later, iOS 7 or later
- **Connectivity:** Reliable broadband internet connection to securely access the cloud-based service
- **Authentication:** Valid user login credentials are required for authenticated platform access
- **Mobile device requirements (for digital ID and Right to Work checks):** NFC capability enabled, front and rear cameras available for selfie and document capture
- **Email access:** Applicants must have access to email to receive invitations and notifications

Aside from NFC-enabled mobile devices for ID verification, no additional hardware is required. Any additional requirements specific to a buyer engagement will be confirmed within the Statement of Work.

2.7 RESELLING

We are not a reseller for the purpose of DBS, however, we are a reselling for other services, for example, Social Media Checks, Digital ID Checks and Right to Work through SP Index and TrustID.

2.8 USER SUPPORT

To give buyers confidence in the reliability of our platform, we provide a structured approach to user support that is designed to keep recruitment processes running without interruption. Ensuring that any queries or issues are handled in a way that maintains compliance and protects vulnerable groups, our model is designed to uphold the DBS Code of Practice and wider safeguarding obligations. We have further aligned our support model to ITIL principles and we deliver this through a combination of self-service resources, multi-channel helpdesk support and escalation pathways to technical specialists.

2.8.1 Support details

Support channel	Details
Email	Standard support available Monday to Friday 9am-5pm. Responses typically within 1 working day
Phone	Direct customer service line available Monday to Friday, 9am-5pm Uk time. Average call answer time within 1 minute 25 seconds, with a target of 30 seconds
Web chat	Accessible through the platform dashboard and support page on the desktop and mobile. An AI chatbot provides initial guidance and triage, with seamless escalation to a human operative during standard support hours (Monday to Friday, 9am-5pm UK time). Outside these hours, a limited automated bot feature remains available 24/7 to provide basic guidance and route queries for follow-up during staffed support hours
WhatsApp	Available for quick queries and applicant guidance during standard support hours

Figure 2.8.1: Support details

For strategic engagements, we provide a dedicated Account Manager to each user, at no additional cost, to support onboarding, change requests and service performance. Ensuring continuity of service, the Account Manager provides monthly check-ins to identify additional support areas. As a point of escalation and ensuring rapid resolution, where a problem cannot be resolved through standard channels, cases are immediately signed to our Director of Operations.

2.8.2 Accessibility and usability

Our service interface and support channels are designed to meet recognised accessibility standards. Reducing barriers, supporting compliance and improving usability for users, our approach includes:

- **Accessibility standards:** The core service interface is designed to meet **WCAG 2.2 AA and EN 301 549 standards**, providing a ready-to-use, compliant solution from day 1. Components provided by third-party partners, such as our LiveChat web chat widget, meets WCAG 2.2 AA, supporting enhanced accessibility. In house documentation, video guides and website content are not fully compliant, however accessibility improvements are actively being reviewed and progressed
- **Accessible design:** We maintain an accessible design through:
    - Intuitive, responsive web-based interface accessible on desktop and mobile devices, enabling flexible use
    - No additional software or plugins required to complete DBS, Right to Work and social media checks, simplifying rollout. For Digital ID verification, an easy-to-use mobile app enables NFC document scanning, providing a fast, secure, and accessible way for users to complete the process
    - Dashboards, progress monitoring and reporting available without barriers
- **Support channel accessibility:** Enabling all users, regardless of digital confidence, can access timely assistance, we provide multiple support channels, including email, phone, web chat and WhatsApp. All interactions logged securely in line with **Cyber Essentials Plus**
- **Documentation formats:** Ensuring that all user guides, manuals and support materials are provided in HTML and PDF formats that meet accessibility guidelines. To address further accessibility needs, alternative formats are available on request
- **Accessibility testing:** In line with section 508, during updates, we conduct automated accessibility checks to maintain compliance. While formal assistive technology testing (for example, screen readers, alternative input devices) may be undertaken by Matrix Security Watchdog, our Service Provider in future releases, we are ensuring all Care Check resources are designed with accessibility principles in mind
- **Customer feedback loops:** Accessibility feedback is actively collected from users and reviewed by the Account Manager during monthly check-ins. Ensuring buyers benefit from ongoing enhancements, any improvements are integrated into subsequent releases as part of our user-centred design process

2.9 HOW USERS WORK WITH OUR SERVICE

2.9.1 Browsers

Ensuring buyers can adopt our platform across diverse IT environments without additional configuration, it is accessible through any standard-compliant web browsers. We support the latest versions of:

- Google Chrome
- Safari
- Microsoft Edge

We recommend enabling JavaScript and cookies for full functionality. Buyers are notified in advance of any changes to browser support.

2.9.2 Desktop application

A dedicated desktop application is not required for our service. All functionality, including DBS applications, digital ID verification, Right to Work checks and social media screening is delivered through a secure, standards-compliant web interface.

For digital ID verification, a small application is required to enable scanning of the passport chip (NFC). This app is only needed for the digital ID process, all other features remain fully web-based.

2.9.3 Mobile

The service is optimised for mobile use and supports access via iOS, Android and Windows devices. Enabling full functionality, users can work through the mobile-responsive web interface. For digital ID verification, the supporting mobile app enables NFC passport-chip scanning where required.

2.9.4 Service interface

Improving recruitment efficiency and reduce administrative workload, our service provides intuitive, web-based interface accessible on both desktop and mobile devices. From a single dashboard, users can submit and monitor DBS applications, digital ID verification, Right to Work checks and social media screenings.

2.9.5 API

- **API availability:** A secure, private API is provided for authorised customers to enable seamless integration with existing systems
- **API capabilities:** Through this integration, customers can:
    - Integrate the platform with their HR/recruitment systems directly
    - Create applicant records and initiate of DBS checks, digital ID verification, Right to Work checks and social media screenings
    - Update applicant details prior to submission, retrieving real-time application statuses and monitors progress
    - Ensure compliance and oversight, all API actions are subject to role-based permissions and are fully logged for traceability
- **Documentation:** Documentation is available in HTML and PDF formats. To support safe configuration and integration testing, we provide a sandbox/test environment before live deployment

2.9.6 Accessibility and useability

Our user interface is designed to meet recognised accessibility requirements, with layouts and navigation selected to support ease of use across different devices. The platform follows and is tested against **WCAG 2.2 AA** principles, ensuring that users with varying needs can interact with the platform effectively.

We place emphasis on useability by applying consistent design patterns across dashboards, search tools and task-based views, helping user's complete activities quickly and confidently. To support inclusivity, the system offers responsive layouts and high-contrast display options. Users can adjust text size using standard browser zoom functionality, providing flexibility for readability across devices.

While formal assistive technology testing and system design updates are managed by the broker, Care Check actively supports accessibility by gathering feedback from users and ensuring that all internal documents and guidance provided are clear, accessible, and aligned with public sector standards.

2.9.7 Customisation

Allowing buyers to tailor the system to their organisational needs, our platform provides a range of configuration options, including:

- **Email templates:** Applicant invitations and notifications can be customised using editable templates. Organisations can tailor wording, instructions and links to reflect internal processes. Visual branding such as logos cannot be applied to the platform interface
- **User roles and permissions:** Role-based access can be configured so users only see data relevant to their branch or function. Head office administrators can manage multi-branch visibility, while branch users remain restricted to their own applicants
- **Workflow and billing rules:** Customers can set up split payment accounts to support different billing arrangements for applicants and organisational-funded checks
- **Dashboards and reporting:** Administrators can generate custom reports using pre-populated templates or define CSV exports to match organisational reporting requirements
- **Notifications:** Ensuring timely communication, progress updates and query alerts can be directed to specific email addresses or roles

All amendments, including templates, notifications, user roles and workflows are implemented by the Care Check team. We provide prompt support, with changes typically completed within 1 working day, ensuring organisations can quickly adapt the service to their processes and compliance requirements. Enabling organisations to adapt the service fully to their internal processes and compliance requirements, all customisation is included at no extra cost.

2.9.8 Service levels and availability

Our Service Level Agreements (SLAs) define the availability, responsiveness and performance standards that apply to our service under the G-Cloud 15 framework. These metrics are monitored continuously, with results reviewed monthly as part of service management reporting. Any breaches of SLA targets trigger internal escalation to the Account Manager, through our Service Provider, including corrective actions. Our ITIL aligned service management framework ensures root cause analysis and continual improvement actions for any SLA breaches. Performance data is logged in real time and reviewed monthly to identify trends and improvement opportunities, ensuring service reliability and continual optimisation.

Metric	Target/guarantee	Action if not met
Platform availability	99% minimum uptime	Service incident investigation and root cause analysis, priority remediation to restore service and communication with customers regarding impact and corrective actions. Where appropriate, preventative measures will be implemented to reduce the risk of recurrence
Recovery Time Objective (RTO)	24 hours	Escalation to Account Manager, through our Service Provider and corrective actions initiated
Recovery Point Objective (RPO)	1 hour	Restoration from latest back up, escalation if exceeded
Incident response times	Critical: <1 hour High: <4 hours Medium: <1 day Low: <3 days	Escalation through incident prioritisation pro

Figure 2.9.8: Defined SLAs

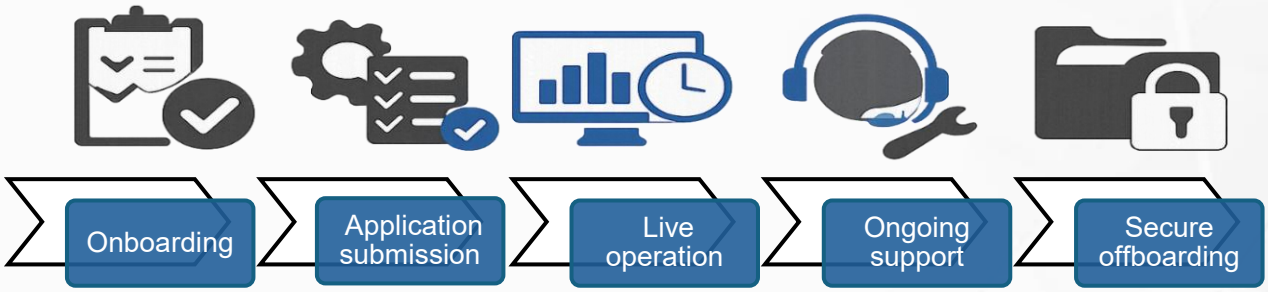
We achieve these SLAs through the following features and processes:

- Supporting rapid restoration within our RTO of 24 hours and RPO of 1 hour, our platform is hosted on UK-based virtual servers with redundant infrastructure and automated failover across geographically separated data centres. Data is backed up multiple times per day, with compressed copies stored securely and OS-level snapshots managed by virtualisation technology.
- Planned maintenance windows are communicated at least 48 hours in advance, with details of expected duration and affected services. Emergency maintenance notifications are issued immediately via email alerts and service notifications. Historical outage reports are available on request for audit and compliance purposes
- Administrators can access real-time dashboards showing application progress, pending tasks, error rates, approvals and per-user/branch activity. All user and system actions are recorded in audit logs. Audit logs show which applications individual users have approved, although this information cannot be exported as a report. Metrics can be exported in CSV format or accessed via API for integration with HR and recruitment systems

3. G-CLOUD ALIGNMENT INFORMATION

3.1 SECTION INTRODUCTION

We deliver every engagement through a tailored, collaborative delivery model that adapts to the specific objectives, scale and governance requirements of each client. This section explains how Care Check and client teams work together at each stage of delivery, beginning with onboarding and configuration, progressing into live operation and support, and concluding with secure offboarding. The diagram below illustrates a typical delivery lifecycle, showing how projects progress through phases, decision points and governance activities.



3.2 ONBOARDING AND OFFBOARDING PROCESSES

3.2.1 Onboarding

Once the contract is signed, onboarding begins with a straightforward registration process:

1. **Registration submission:** Buyer completes the registration form
2. **Review:** Registration is checked, including a credit review
3. **Setup:** Accounts are created, users added, and login details with a welcome pack are issued
4. **Training (optional):** Online or guided training sessions are available

Customers are typically set up within 30 minutes during office hours. Where multiple branches are requested and users need linking across sites, setup may take longer depending on volume. To support rapid onboarding, Care Check provides user guides, video tutorials and online manuals accessible from desktop, tablet or mobile without additional software. Documentation covers DBS, digital ID, Right to Work and social media checks, reducing errors. Guidance is tailored to user roles, helping administrators and branch staff follow correct procedures while maintaining compliance with DBS Codes of Practice.

3.2.2 Offboarding

To ensure a smooth transition and sustained value after delivery, every engagement concludes with a structured offboarding phase. Typical offboarding steps include:

1. **Notification of exit (optional):** Whilst our terms do not require formal notification when a customer leaves, we encourage buyers to inform us so that system access can be removed promptly and securely
2. **Data extraction:** Buyers can obtain their data at any time using the custom report function, which provides outputs in CSV format for integration with other systems

3. **Data availability and cleansing:** Full data for applications completed within the last 6 months is provided. In line with DBS Codes of Practice, snapshot/result data and selected personal information older than 6 months are partially retained and cleansed to ensure compliance
4. **Access revocation:** Once offboarding is confirmed, all user accounts and system access are revoked to maintain security
5. **Restrictions:** The only circumstance in which data downloads may be limited is where outstanding account balances remain unpaid
6. **Optional services**: Any services outside the standard contract scope, excluding custom reporting, which cannot be provided due to system limitations, are agreed separately and may incur additional cost and are subject to system availability

3.3 DATA

3.3.1 Data importing and exporting

Ensuring buyers retain full control of their information, with no vendor lock in, the service supports flexible, standards-based data import and export. Our approach includes:

- **Data importing:** Buyers can upload applicant information in CSV format, using the set template provided, which is the standard for bulk data entry and integration with HR or recruitment systems
- **Data exporting:** Ensuring seamless operational continuity, users can export their data using the platform's custom report function, which generates CSV files for integration with other systems. A PDF export option is also available, limited to 50 records per PDF sheet. Supporting efficient record-keeping, full data for applications completed within the last 6 months are readily available in line with DBS Codes of Practice. Facilitating regulatory adherence, snapshot and personal data older than 6 months are partially retained, with sensitive results removed while essential identifiers remain. Maintaining secure and controlled access, users can initiate exports independently through their dashboard at any time, with no additional cost under the standard contract
- **End-of-contract extraction:** At contract end, buyers can extract all applicant data through the custom report function in CSV format. In line with DBS Codes of Practice, data for applications completed within the last 6 month is fully available while older records are partially cleansed. Fully anonymised or deleted records are permanently removed after 6 years, in accordance with data-protection requirements

3.3.2 Analytics

Our platform provides built-in analytics that gives buyers meaningful and actionable insight into usage and performance data. Buyers can monitor:

- Application progress
- Pending tasks
- Approvals

To track progress and activity, administrators can use real-time dashboards. Enhancing reporting, metrics can be exported in CSV format or accessed via API for integration with HR and recruitment systems.

3.3.3 Independence of resource

Ensuring strict separation between buyers, our service is delivered through a secure multi-tenant architecture. Ensuring each organisation's data remain isolated, we enforce strict role-based access. For example, multi-branch access controls support operational efficiency, enabling head office oversight while restricting branch users to their own applicants. Preventing activity from one buyer impacting the other, compute, storage and network resources are automatically scaled and load balanced. Maintaining consistent performance regardless of wider platform demand, we use resource isolation, prioritisation controls and automated capacity management. Ensuring high demand does not impact wider service availability, reporting, API access and metrics extraction are processed per organisation.

3.3.4 Public sector networks

The service does not require direct connectivity to public sector networks for operation.

3.3.5 Data-in-transit protection

All data transmitted to and from the service is protected using industry-standard **TLS 1.2+** encryption, ensuring confidentiality and integrity. Secure API gateways enforce strong authentication and access controls.

3.3.6 Asset protection

Customer information is hosted exclusively within UK-based data centres that meet recognised security certifications, including **ISO 27001** and **CSA Cloud Controls Matrix.** In addition, Care Check also holds **Cyber Essentials Plus** certification, demonstrating adherence to UK government-backed security controls. Data stored at rest is safeguarded with **AES-256** encryption and each user's information is kept separate through strict role-based permissions and logical environment segregation.

When data is deleted, it cannot be retrieved. Erasure is carried out using cryptographic methods that ensure permanent removal in line with industry best practice. Guaranteeing that no residual data remains and compliance with security obligations is maintained, hardware that reaches end-of-life is disposed of under approved destruction processes.

3.4 AVAILABILITY AND RESILIENCE

3.4.1 Guaranteed availability

Our platform is hosted on UK-based virtual servers with redundant infrastructure and automated failover across geographically separated data centres. Ensuring resilience against localised outages, our application and database servers operate in 2 separate UK locations. This includes a primary data centre and a secondary site used for disaster recovery and business continuity.

Data is backed up several times per day, with compressed copies stored securely within the same network zone. Enabling rapid restoration, additional file and OS-level snapshots are managed by the data centre's virtualisation technology. Ensuring minimal disruption in the unlikely event of an incident, recovery objectives are defined as an RTO of 24 hours and an RPO of 1 hour.

System health and uptime are continuously monitored, with automated alerts enabling rapid response to potential issues. We guarantee a minimum SLA of **99%** uptime for platform infrastructure.

3.5 GOVERNANCE

Service delivery is managed under an integrated governance framework aligned to recognised industry standards. Evidencing compliance with UK government-backed security controls, we hold **Cyber Essentials** certification. Processes for service management are structured around ITIL v4 principles, ensuring continual improvement and effective incident handling.

To identify opportunities for improvement, Danielle Pinner, Director of Operations reviews platform performance metrics, customer feedback and internal audit findings monthly. Providing further assurance that our platform operates professionally, we undergo annual external audits as part of Cyber Essentials Plus certification, conducted by IASME Consortium Ltd. Ensuring quality, security and risk management remain central to service delivery, oversight of compliance and governance activities is provided by our Senior Management Team.

3.6 SECURITY GOVERNANCE

Security is embedded across all operations and governed through a comprehensive suite of policies, including our:

- Data Protection Policy
- Information Security Policy
- Data Processing Agreement
- Data Retention Policy
- Data Breach Policy
- Appropriate Use Policy

To ensure we remain aligned with our **Cyber Essentials Plus** accreditation, our policies are reviewed annually. To reinforce compliance, all staff receive training on these policies during induction and refreshed regularly. Oversight of security governance is provided by Charles Eason, Managing Director, who is accountable for governance, risk management and compliance activities.

3.6.1 Operational security

Configuration and change management	Ensuring that our infrastructure is securely developed, deployed and maintained, we operate a robust configuration and change management framework that governs all platform components throughout their lifecycle. To maintain service availability and compliance, all platform components, including virtual servers, applications and sub-processor integrations, are tracked throughout their lifecycle from deployment to decommissioning. Our Service Provider is responsible for maintaining up-to-date change management processes. All proposed changes are assessed for security, operational and regulatory impact before implementation. Emergency changes require our Service Provider's approval and are subject to immediate post-implementation review. For traceability and accountability, all configuration changes are logged in the Service Provider's Information Security Management System, providing a complete audit trail for compliance and post change analysis.
Protective monitoring	To safeguard user data and maintain operational continuity, our platform employs continuous monitoring across all virtual servers, applications

	and sub-processor integrations. Potential compromises are detected through anomaly identification, enabling rapid containment of threats before they escalate. Prioritising incidents based on severity, our Service Provider is accountable for investigating alerts and implementing corrective actions immediately. Supporting regulatory compliance, accountability and post-incident review, we log all activity and responses in our internal file structure, following discussions with our Product Manager.
Incident management	Our incident management framework is designed to deliver rapid response and minimise disruption. Pre-defined procedures exist for common events such as system outages, data access issues and security incidents, ensuring consistent and efficient handling. Users can report incidents via email, phone or web chat, with clear guidance provided on severity and required details. All incidents are logged and tracked in our Service Provider's Information Security Management System, including investigation outcomes and corrective actions. Following resolution, users receive incident reports outlining the cause, impact, remediation steps and lessons learned.

Figure 3.6.1.1: Operational security

3.6.2 Staff security

All employees with access to systems or customer data undergo thorough background checks in line with recognised standards such as **BPSS/BS7858:2019**. Ensuring that only appropriately vetted staff are authorised, these checks cover identity verification, employment history and criminal record disclosure. Access privileges are granted strictly on a least-privilege basis, meaning individuals can only reach the information necessary for their role. This is enforced through role-based access controls, multi-factor authentication (MFA) and detailed activity logging, providing full visibility and accountability for system use.

3.6.3 Secure development

Our platform is developed and maintained in line with recognised secure development standards, including **ISO 27001** and **CSA CCM v4.0**. Security is embedded throughout the software development lifecycle, including threat modelling, code review, adherence to secure coding standards and automated security testing tools. To confirm the strength of these controls and demonstrating ongoing compliance with industry requirements, we commission independent assessments on a regular basis. These include penetration testing and structured secure development audits, providing assurance that vulnerabilities are identified promptly and remediated effectively.

3.6.4 Identify and authentication

User access is controlled through strong authentication options:

- **Role-based access control (RBAC):** Users are assigned permissions according to their role, ensuring they only access applicants and data relevant to their responsibilities
- **Principle of least privilege:** Access rights are limited strictly to the functions required for each job role
- **Secure login credentials:** All platform interfaces require authenticated access with password policies aligned to recognised standards. MFA is enabled by default for Care Check staff and can be activated on request for individual customer accounts, giving organisations the option to apply it where required

- **Access monitoring and audit logs:** All login attempts and actions within management interfaces are logged, supporting accountability and compliance

3.7 AUDITING

Our platform maintains comprehensive audit logs that capture all significant user and system activity, including authentication events, data changes and administrative actions. Every access to the system is fully logged with time and date stamps, creating a complete audit trail for accountability. To support continuous monitoring, audit data is retained for at least 12 months, depending on buyer requirements, ensuring sufficient history is available for investigation, reporting and regulatory purposes. For data extraction, customers can use our custom reporting function, which provides audit information in CSV format for easy integration into other systems.

3.7.1 Performance monitoring and metrics

Drawing on our **23 years'** experience and to deliver a high-quality service, we will implement a performance management framework including:

- **Continuous monitoring:** Ensuring rapid response to issues, the platform is continuously monitored using automated tools that track availability, response times, error rates and transaction volumes. Alerts are generated immediately if thresholds are breached, enabling swift intervention
- **Defined reporting intervals:** Providing buyers with confidence in service stability, performance data is reviewed at daily, weekly and monthly intervals. These structured reviews identify trends, validate service health and highlight opportunities for improvement
- **Meaningful metrics for buyers:** Providing buyers with transparency, usage and performance metrics are made available through dashboards. This includes application progress, completion times, pending tasks and system availability
- **Audits:** Supporting compliance and audit requirements, all monitoring data is retained and can be shared with buyers on request, ensuring traceability and confidence in service delivery

3.7.2 Compliance and quality management

Our platform is delivered using an **ISO 27001**-certified system and our internal processes operate in alignment with **ISO 9001**, **ISO 27001** and **ISO 22301** principles. As an organisation, we are actively working towards achieving full ISO 27001 certification by mid 2026. Facilitating consistent standards, we also maintain a **Cyber Essentials Plus** and structure our service delivery around ITIL v4 practices. To identify areas for enhancement and to monitor progress of corrective actions, we review service performance data, customer feedback and audit outcomes on a monthly basis. Oversight of these management systems is provided by our Director of Operations who reports directly to the organisation's Managing Director, ensuring accountability and governance at the highest tier.

3.8 BACKUP, RESTORE & DISASTER RECOVERY

To safeguard all applicant and customer information assets, we maintain comprehensive Data Protection, Business Continuity and Information Governance policies. Maintaining service continuity, data integrity and minimal disruption to customer operations, our

approach follows established best practices in information security and business continuity management and is supported by our **Cyber Essentials Plus accreditation**.

Overview and governance	Our Business Continuity Management (BCM) framework identifies potential threats, evaluates their impact and defines structured response procedures. In the event of disruption, our Managing Director (covered by our Director of Operations during absence) initiates recovery protocols, manages communications and oversees restoration of services. We conduct a full risk assessment bi-annually and test resilience through scheduled continuity and disaster-recovery exercises.
Backup and data protection	Promoting resilience and data integrity, database backups run automatically several times per day. Standard database tools generate compressed backup files, which are securely copied to a file system within the same protected network zone. Our data centre's virtualisation technology also creates additional file operating system-level snapshots, which are managed by internal operations teams manage to maintain reliability and consistency. Application and database servers are hosted across two geographically separate UK data centres, providing redundancy and high availability. Enabling rapid restoration of services if the primary facility is disrupted, the secondary data centre functions as a disaster recovery and business continuity site.
Disaster recovery and restoration	In the event of disruption, our Disaster Recovery Plan sets out recovery priorities and escalation procedures. Our defined objectives are to: • Restore essential systems within 24 hours • Limit potential data loss to less than one business day • Maintain continuous communication with client contacts throughout recovery • Where local data loss could occur, we prompt users immediately to back up personal workstations, ensuring all operational information is captured and restored
Continuous improvement and assurance	Following every exercise or live incident, we carry out a structured review and incorporate the insights gained into revised procedures. This continuous improvement model enhances resilience and maintains full compliance with ISO 22301 and the framework terms.

Figure 3.8.1: Our Data Protection, Business Continuity and Information Governance policies

3.9 TRAINING

Ensuring organisations can adopt and sustain our platform with confidence, we embed training and knowledge transfer as a core element of our onboarding and throughout service delivery. Training is available in multiple formats to suit different user needs:

- **Online sessions:** Delivered either one-to-one or in group format, covering workflows, compliance requirements and system functionality
- **Online manuals and video tutorials:** Step-by-step guidance that enables users to navigate DBS, digital ID, Right to Work and social media checks independently
- **Telephone support:** Direct access to trainers who can explain processes, answer questions and reinforce confidence in using the system

Beyond onboarding, we offer ongoing training options, which may include:

- Refresher sessions for administrators and HR teams
- Train-the-trainer programmes to build in-house expertise
- Bespoke workshops to support integration with HR or recruitment systems, multi-branch access, and configuration of notifications or reports

To further self-sufficiency, we provide online manuals, video tutorials and step-by-step guidance, ensuring users can navigate DBS, digital ID, Right to Work and social media checks independently. All training, demonstrations and documentation is included within our pricing. Promoting continuous improvement and sustained adoption, we measure effectiveness through participant feedback.

3.10 SERVICE PRICING

Enabling flexibility for organisations of different sizes, our service is priced on volume-based mode. Customers are encouraged to contact us to discuss their specific requirements, as pricing can be adjusted depending on usage levels and organisational factors. Discounts are available for organisations processing more than 100 checks per year, with the following bands:

- 101-200 checks
- 201-500 checks
- 500+ checks

For larger volumes, we can reduce pricing further following direct discussion with the customer. We do not apply charges for customisation, training, storage or standard support. Additional charges only apply where customers request optional services such as digital ID verification, Right to Work checks or social media checks. An annual fee applies if customers choose to use the optional update service checking facility.

We do not offer free trials. However, customers can be provided with access to a demonstration system to view and understand how the service operates. In limited circumstances, such as for very large contracts, a small number of free checks may be agreed on a case-by-case basis.

Full pricing details are provided in the separate Pricing Document published on G-Cloud.

3.11 INVOICING PROCESS

Flexible invoicing terms	We offer flexible invoicing options to meet different customer requirements: • **Pay-as-you-go:** Customers may pay by credit/debit card prior to submitting an application • **Per-application invoicing:** Invoices can be issued at the point an application is approved • **Monthly invoicing:** Customers may choose consolidated monthly invoicing in arrears for all checks completed during the billing period
Payment terms	• Standard terms are 15 days from invoice date, although we can accommodate the government's standard 30-day payment terms where required and alternative terms may be considered subject to discussion and agreement • We accept payment via BACS transfer, purchase order (PO), or credit card
Minimum contract or billing period	• No minimum contract period applies for the core service • Customers who opt for the update check service facility enter into a separate annual contract with yearly billing

Figure 3.11.1: Invoicing process

3.12 TERMINATION

Termination is governed by the Crown Commercial Service G-Cloud 15 Call-Off Terms and Conditions. Buyers may terminate the contract in accordance with these terms by providing

written notice. Care Check may terminate only in cases of material breach, non-payment or where the service is used in a manner that breaches DBS rules, applicable law. Upon termination, all data will be handled in line with our offboarding and data-deletion process described in Section 3.2.2 Offboarding.

4.SECURITY AND DATA GOVERNANCE

4.1 DATA PROTECTION AND ENCRYPTION

To ensure the confidentiality, integrity and availability of data, we apply robust encryption protocols to protect all sensitive data, both at rest and in transit, using **TLS 1.2** or above encryption. As a **Cyber Essentials Plus** certified organisation, we follow best practices aligned with **National Cyber Security Centre** guidance and principles.

Our infrastructure is protected by layered security controls, including firewalls, intrusion detection, network segmentation and strict role-based access policies. Application and database servers are hosted in secure UK data centres with strong physical and logical access controls.

Encryption keys are managed through secure key-management processes with restricted access, regular rotation and audit logging. Continuous monitoring tools detect anomalous activity in real time, with alerts escalated to our operations team for immediate investigation.

While post-quantum cryptography is not yet mandated for DBS-related services, our encryption standards follow current NCSC guidance and will be updated as standards evolve. Care Check plans to be fully compliant with post-quantum requirements within the next 24 months and will implement a transition plan within the next 12 months. This transition will follow NCSC Post-Quantum Cryptography (PQC) guidance and adopt trusted implementations of the ML-KEM and ML-DSA cryptographic algorithm standards.

4.2 DATA AT REST, STORAGE LOCATIONS AND PHYSICAL SECURITY

All data at rest is encrypted using **AES-256**, ensuring strong protection against unauthorised access. Data is stored exclusively within accredited UK data centres that comply with **ISO 27001** and recognised security and resilience standards. To protect systems from physical intrusion, data-centre facilities include 24/7 manned security, CCTV monitoring, biometric access controls, and perimeter protection.

4.3 DATA SANITISATION AND DISPOSAL

Data is securely sanitised in line with NCSC and industry best practice. Deleted data is rendered irrecoverable using cryptographic erasure or secure overwrite methods prior to storage reuse or system decommissioning. To ensure no residual data remains and security obligations are met, hardware that reaches end-of-life is disposed of through approved destruction processes operated by our accredited UK data-centre providers.

4.4 SECURITY TESTING AND ASSURANCE

To ensure ongoing protection against emerging threats, we maintain a rigorous security testing and assurance programme. This includes:

- Annual penetration testing carried out by independent, accredited specialists. Maintaining strong security controls, we review all findings and remediate promptly.
- Regular automated vulnerability scanning across our hosted infrastructure to identify weaknesses before they can be exploited
- Prioritised remediation workflow, ensuring high-severity issues are addressed promptly and lower-risk items are resolved within defined maintenance cycles

- Routine configuration reviews and patching, keeping operating systems, application frameworks and third-party components up to date and secure
- Secure data sanitisation using cryptographic erasure or secure overwrite methods before storage media is reused or systems are decommissioned by our accredited UK hosting provide
- Accredited hardware disposal carried out by certified third-party destruction providers used by our UK data-centre partners

4.5 INCIDENT AND PROTECTIVE MONITORING MANAGEMENT

To minimise disruption, our incident-management framework follows pre-defined procedures for common events such as system outages, data-access issues and security incidents. Users can report incidents via email, phone or web chat, with clear guidance provided on severity levels and required information. All incidents are logged, tracked and managed within our incident-management system, including investigation outcomes and corrective actions. Following resolution, users receive an incident report outlining the cause, impact, remediation steps and lessons learned.

To safeguard user data, our platform employs continuous monitoring across all virtual servers, applications and approved sub-processor integrations. Enabling rapid containment of threats before they escalate, this monitoring identifies anomalies that may indicate potential compromise. Incidents are classified and prioritised by severity, with our dedicated security and operations team responsible for investigating alerts and implementing corrective actions immediately. All monitoring activity and responses are logged by our Service Provider, supporting regulatory compliance, accountability and post-incident review.

4.6 CONFIGURATION AND CHANGE MANAGEMENT

To ensure our platform is securely developed, deployed and maintained, we operate a robust, ITIL-aligned configuration and change-management framework governing all components throughout their lifecycle.

For full traceability, all platform elements, including virtual servers, applications and approved sub-processor integrations, are tracked from deployment through to decommissioning by our Service Provider. Assigning responsibility, our Service Provider Team is accountable for maintaining up-to-date change-management processes. All proposed changes undergo security, operational and regulatory impact assessment before implementation and our Service Provider ensures changes follow controlled deployment steps, including testing and validation.

Emergency changes are managed by our Service Provider and are subject to immediate post-implementation review to confirm stability and compliance. For accountability, all configuration and change activities are logged in the Service Provider's Information Security Management System, providing a complete audit trail for compliance and post-change analysis.

4.7 INFORMATION SECURITY MANAGEMENT AND CERTIFICATIONS

Highlighting the strength of our governance framework and third-party validation, Care Check:

- Hold **Cyber Essentials Plus accreditation**

- Undergo annual external audits as part of Cyber Essentials Plus certification, conducted by IASME Consortium Ltd
- Conduct penetration testing, completed by a CREST-approved service provider for the main system, with in-house testing performed on internal systems
- Are overseen by a Data Protection Officer, who is responsible for policy governance, risk management and incident oversight

4.8 SECURE DEVELOPMENT AND CRYPTOGRAPHY

Embedding security controls from design through to deployment, our platform is developed using a secure development lifecycle (SDLC). All code changes undergo peer code reviews, static analysis and automated dependency scanning to identify vulnerabilities, outdated libraries and supply-chain risks before release.

All sensitive data is protected using strong, industry-standard cryptographic controls. Data in transit is encrypted using **TLS 1.2 or above** and data at rest is encrypted using **AES-256**. Encryption keys are managed through secure key-management processes with restricted access, rotation and audit logging.

While post-quantum cryptography is not yet mandated for DBS-related services, our encryption standards follow current NCSC guidance and will be updated as standards evolve. Care Check plans to be fully compliant with post-quantum requirements within the next 24 months and will implement a transition plan within the next 12 months. This transition will follow NCSC Post-Quantum Cryptography (PQC) guidance and adopt trusted implementations of the ML-KEM and ML-DSA cryptographic algorithm standards.

4.9 IDENTITY AND ACCESS MANAGEMENT

To prevent unauthorised access, users and administrative access to the platform is governed by strict identity (usernames and passwords) and access-management controls. Access to system functions and data is controlled through role-based access control (RBAC), ensuring users only have the permissions required for their role. Privileged actions are restricted to authorised personnel and fully audited.

5. SUPPLIER INFORMATION

5.1 ABOUT US

Care Check is one of the UK's longest-established and most trusted Disclosure and Barring Service (DBS) providers, supporting organisations nationwide for more than **20 years**. Founded in 2002, at the introduction of the DBS (formerly CRB), we have grown from a paper-based checking service into one of the largest and most efficient digital DBS providers in the country.

Today, we process over **200,000** Basic, Standard and Enhanced DBS checks every year for more than **45,000** organisations. These range from small businesses and charities to major national employers across:

- Healthcare
- Education
- Construction
- Social care
- Transport
- Police
- Public order and safety

Care Check was among the first umbrella bodies to adopt electronic eBulk submissions in 2009 and we continue to lead the market in digital transformation. Our secure cloud-based platform provides DBS checks alongside complementary services such as:

- Digital ID verification
- Right to Work checks
- Social media checks

At the heart of our service is a commitment to delivering exceptional value, transparency and trust. We believe in making compliance simple, affordable and accessible for every organisation. Our core values guide how we operate and support our customers:

- Affordability without compromise
- Transparency and fairness
- Customer-centric excellence
- Innovation and simplicity
- Security and compliance first
- Local and sustainable

We are committed to the highest standards of security and resilience, holding a **Cyber Essentials Plus** accreditation.

5.2 RELEVANT EXPERIENCE AND TESTIMONIALS

Demonstrating consistent, high-quality service delivery, Care Check has built a strong reputation for reliability, responsiveness and customer care across multiple clients including:

Our commitment to service excellence is reflected in independent customer feedback on Trustpilot:

"We have been working with Care Check for several years now for our DBS requirements. We had a slight problem with something today and I called, got through immediately and spoke with an advisor. Within a couple of minutes everything was resolved and we were able to continue processing our applicant. Very quick customer care and service. Well done!"

"I have become so accustomed to poor customer service that unfortunately, have accepted that it is the norm to be treated as if it doesn't matter anymore. Well... Care Check has restored my faith that it DOES matter! I emailed with a query regarding an application made, but I couldn't see. They responded in a couple of hours with a positive 'can do' attitude, requesting further information. My query was resolved same day. I really got the impression that they understand the importance of providing a timely service and didn't feel like I was interrupting their day with my request. THANK YOU, it was a pleasure dealing with you."

"I have always found this company to be very efficient and super helpful and will continue to use them in the future Very patient with all questions that have been asked."

"Incredibly professional services, easy to use, thorough, and reliable. I am especially impressed by their level of customer service, fast replies, and willingness to help. Highly recommended!"

5.3 HOW TO BUY

Care Check's services can be procured directly through the Crown Commercial Service (CCS) **G-Cloud 15 Digital Marketplace**. Public-sector buyers can locate our service by searching for **Care Check** on the Digital Marketplace and selecting the relevant service listing. Once selected, the procurement process follows the standard G-Cloud call-off procedure:

1. **Agree a Statement of Work (SOW)** outlining the service scope, deliverables, timescales and pricing
2. **Raise a Call-Off Contract** under the G-Cloud 15 framework terms
3. **Issue a Purchase Order (PO)** to confirm commencement of services

CareCheck

Care Check Ltd
1st Floor Orchard House,
Crab Apple Way, Vale Park, Evesham, WR11 1GE