Scanning & Digitisation

Service Definition

G-Cloud 15

Contents

1 Overview

Capita's Scanning and Digitisation service is designed to help public sector organisations transform both physical documents and digital files including emails and electronic records into secure, accessible digital assets. The core focus is on digitisation: converting information from paper and electronic sources into formats that can be easily managed, searched, and used across the organisation. This process enables rapid access to data, supports compliance with government and regulatory standards, and streamlines workflows for remote and hybrid working.

While archiving is an important aspect, allowing organisations to preserve records for the long term and meet legal or regulatory requirements the primary value lies in the digitisation process itself. Capita's solution integrates paper and digital records into unified archives, but it is the digitisation capability that drives efficiency, improves responsiveness to data requests, and ensures robust information governance.

The service is delivered in secure, UK-based, ISO-certified environments and aligns with government expectations for data protection, business continuity, and legal admissibility. It is ideal for any public sector organisation seeking to manage, preserve, and access both physical and digital records securely and compliantly.

Legal Admissibility: Digitised outputs are managed under BS 10008 procedures with auditable integrity controls, enabling evidential acceptance where applicable.

1.1 Service Description

Capita's Scanning and Digitisation service is a comprehensive solution that transforms physical documents and digital files, including emails and electronic records, into secure and accessible digital assets. The service provides a unified platform where all information, regardless of its original format, can be managed, searched, and used efficiently.

All processing takes place within secure UK-based environments certified to all relevant ISO standards (See Section 1.6), ensuring the highest levels of data security, legal admissibility, and compliance with government requirements. Capita uses advanced data extraction, automation, and AI-enhanced capabilities to help organisations classify, mine, and act on information quickly and accurately. This includes intelligent document processing for classification, metadata extraction, and sentiment analysis, enabling automated triage, routing, and case creation for high-volume environments.

Regular automated backups and robust disaster recovery are included as standard, supporting business continuity and peace of mind. The service is scalable and supports both large projects and ongoing operational needs, with seamless integration into existing systems. Onboarding and offboarding are rapid and straightforward, ensuring minimal disruption.

1.2 Business Continuity and Disaster Recovery

Capita's service is designed to protect your data and maintain operational continuity through robust backup and recovery measures.

- All data is automatically backed up at regular intervals, with secure, geographically separate UK-based storage.
- Disaster recovery plans are in place to restore services quickly and minimise downtime in the event of disruption.
- Regular failover testing ensures critical data and systems can be recovered efficiently.
- Measures are supported by ISO 22301 certification for business continuity management and align with government best practice.

- Recovery time objectives (RTO) and recovery point objectives (RPO) are clearly defined and communicated.
- Systems are monitored 24/7, with rapid incident response and ongoing support from Capita's dedicated teams.

Business Continuity & Disaster Recovery Timeline

Capita operates an established BC/DR framework that ensures continuation of services in the event of an unplanned incident. Standard BC/DR is provided as part of the core service, with Enhanced DR available as an optional upgrade. The framework includes incident assessment, tactical and operational recovery, controlled work restoration, and structured client communication.

1. Standard BC/DR Provision

1.2.1 Immediate Incident Response

- Rapid evaluation of incident impact and staff safety.
- Incident Management (IM) team convenes to assess severity, likely duration and immediate risks.
- Site security established; evacuation initiated where necessary.
- Emergency services or specialist contractors contacted as required.

1.2.2 Stabilisation & Command Structure (1–4 hours)

- IM team confirms responsibilities and activates command and communication structure.
- Consideration of DR site deployment, equipment relocation and inbound mail redirection.
- Tactical team begins work recovery planning.
- Strategic communication initiated to internal stakeholders.

1.2.3 BC/DR Invocation (4–24 hours)

- Formal invocation of BC/DR plans based on assessed impact.
- Operations and IT preparation at the DR site.
- Work-in-progress (WIP) recovery begins from the point of incident.
- Client communication initiated *only where service levels are at risk*.
- Regular updates issued to staff and clients as appropriate.

1.2.4 Recovery Operations (24–72 hours)

- Production transitions to the DR site if required.
- Materials and supplier adjustments actioned (redirection/replenishment).
- WIP recovery continues with prioritisation aligned to client needs.

- Work recovery plans agreed and executed.
- Ongoing monitoring of service stability.

1.2.5 Stabilisation Phase (3–7 days)

- Restoration work begins at the affected site.
- Plans refined to meet client expectations and workload priorities.
- Continued WIP recovery; clients may be asked to resend unrecoverable data.
- Regular client updates provided through the nominated point of contact.

1.2.6 Return to Business-as-Usual (Day 8 onwards)

- Production resumes at the restored primary site.
- All in-scope work processed and dispatched per normal schedules.
- Outstanding WIP cleared and MI/audit trails fully recovered.
- Work migrated back from DR site; DR activity closed down.
- Continued reporting until full-service normalisation.

2. Client Responsibilities

- Maintain standard data submission processes during a BC/DR event.
- Provide a nominated single point of contact for BC/DR communication.
- Support agreed SLA relaxation where required due to major incidents.
- Resend data where specific WIP items cannot be recovered.

3. Communication Approach

- Capita will contact clients **only** when work is impacted or SLA thresholds are at risk.
- Updates are provided at an agreed frequency through the nominated contact.
- Clear, concise, and auditable records of communications are maintained.

4. Optional Enhanced DR

Enhanced DR can be provided on a per-client basis, offering:

- Accelerated recovery times.
- Pre-positioned infrastructure capacity.

- Bespoke RTO/RPO targets.
- Dedicated DR environments.
- Tailored communication protocols.
- Extended operational cover.

5. Restoration and Audit Assurance

Enhanced DR is scoped and costed individually as part of onboarding or service expansion.

- All BC/DR activity is fully audited.
- MI, processing logs, and audit trails are restored and verified.
- Post-incident reviews conducted internally and with clients (if required).
- Lessons-learned outputs feed into continuous service improvement.

6. Alignment to ISO & Security Frameworks

Capita's BC/DR operations align with:

- ISO 27001 Information Security Management
- ISO 22301 Business Continuity Management
- ISO 9001 Quality Management
- NCSC Cloud Security Principles
- GDPR and UK Data Protection Act requirements

BC/DR Recovery Timeline Table (Standard Provision)

Phase	Timeframe	Key Activities	Client Impact / Expectations
Immediate Incident Response	Not time-bound	- Assess incident impact and staff safety - IM team convenes - Secure or evacuate site - Engage emergency services if required	- No contact expected - Operations may be paused
Stabilisation & Command Setup	1–4 hours	- Establish command structure - Consider DR site deployment - Begin tactical recovery	- Unlikely to be contacted unless severe

		planning - Assess inbound mail redirection needs	- No change to normal data submission
BC/DR Invocation	4–24 hours	- Formal BC/DR activation - Prepare operations and IT at DR site - Begin WIP recovery - Begin controlled client communications	- Will be contacted only if SLAs risk breach - May receive situation updates
Recovery Operations	24–72 hours	- Transition work to DR site - Redirect/replenish materials - Continue WIP recovery - Agree recovery plans with clients	- Possible service disruption - May be asked to resend unrecovered WIP
Stabilisation	3–7 days	- Begin restoration at affected site - Adjust plans to priorities - Continue WIP recovery - Provide regular updates	- Ongoing communication - Gradual service return
Return to BAU	Day 8 onwards	- Resume production at main site - Clear remaining WIP - Restore MI/audit trails - Close DR operations	- Full service normalisation - Final update provided

RTO / RPO Summary (Standard Provision)

Metric	Standard BC/DR	Notes
RTO (Recovery Time Objective)	Defined by incident severity; aligned to phased recovery windows	Enhanced DR can accelerate
RPO (Recovery Point Objective)	Recovery begins from time of incident; unrecoverable WIP may require resubmission	Client resend may be required
Service Restoration Point	Full BAU typically resumes from Day 8 onwards	Subject to incident severity

1.3 Support

Capita is committed to providing ongoing support to ensure customers receive timely assistance and reliable service throughout their engagement.

1.3.1 Onboarding Support

Capita provides comprehensive onboarding support to ensure a smooth and efficient start for new customers. Dedicated teams guide organisations through initial setup, data migration, and integration with existing systems. Clear documentation and training are provided to help users become familiar with the service and its features. Throughout the onboarding process, Capita offers responsive assistance to address any queries or technical requirements, ensuring organisations can begin using the service confidently.

1.3.2 Ongoing Support

Capita offers ongoing support throughout the duration of the service. Customers have access to a UK-based helpdesk for technical assistance, incident management, and service queries. Support is available during standard business hours (Monday–Friday, 09:00–17:00) excluding England bank holidays, with options for extended coverage if required. Regular service reviews, proactive monitoring, and transparent communication ensure that any issues are addressed promptly and that the service continues to meet organisational needs. Capita's commitment to ongoing support helps maintain high levels of satisfaction and operational continuity.

1.3.3 Offboarding Support

When a customer chooses to exit the service, Capita delivers secure and transparent offboarding support. All data is made available for extraction in agreed formats, with clear processes for transfer and deletion to ensure compliance with data protection regulations. Capita's teams provide guidance throughout the offboarding process, helping organisations manage the transition and maintain continuity. Secure handover and confirmation of data removal are standard, giving customers peace of mind that their information is handled responsibly.

1.4 Service Constraints and Customisation

The service operates within defined parameters to ensure reliability, security, and compliance while offering flexibility where possible.

- Scheduled maintenance windows are communicated in advance to minimise disruption and ensure service reliability.
- Customisation options are available within defined parameters to maintain security, compliance, and service integrity.
- Major system changes or upgrades are planned outside of core business hours whenever possible.
- Some aspects of the service, such as core security controls and data handling processes, are standardised and cannot be customised.
- Requests for additional features or integrations are assessed on a case-by-case basis and may be subject to feasibility and approval.
- Service availability and performance may be temporarily affected during planned maintenance, with advance notice provided to all customers.

1.5 Service Levels and Performance

Capita is committed to delivering consistently high standards of performance and reliability, ensuring customers can access their information when needed and receive timely support. The service is designed to meet agreed availability targets, with regular monitoring to maintain optimal performance.

Real-Time Monitoring and Automated Alerts

- Continuous monitoring of services and infrastructure to detect issues early.

- Automated alerts ensure problems are flagged and resolved before they impact delivery.

Predictive Data Analysis

- Advanced analytics to anticipate customer needs and enable proactive engagement.
- Dynamic rule-based communication tailored to customer profiles.

Proactive Change Management

- Structured processes for configuration, release, and deployment changes.
- Updates tested in non-production environments with back-out plans to minimise risk.

Risk Management and Audit Processes

- Embedded audit processes to identify improvements and maintain compliance.
- Strong governance aligned with ISO standards.

1.6 Security

Capita's Scanning and Data Extraction service is designed and operated under a **Secure by Design** approach, fully aligned with **NCSC Cloud Security Principles** and **GovAssure CAF outcomes**. The service is delivered within UK-based, ISO-certified environments and adheres to the following recognised standards and certifications:

- **ISO 27001** (Information Security Management)
- **ISO 27017** (Cloud Security Controls)
- **ISO 27018** (Protection of Personally Identifiable Information in Cloud Services)
- **ISO 22301** (Business Continuity Management)
- **ISO 9001** (Quality Management)
- **Cyber Essentials Plus**

BS 10008 Evidential Integrity: Digitised records are created and managed in accordance with BS 10008, maintaining evidential weight through controlled capture, documented chain-of-custody, hash-based integrity checks, tamper-evident audit trails, and sampling-based quality control. Procedures and artefacts (e.g., integrity reports and audit logs) are available to support legal admissibility.

Personnel Screening and Training:
Staff handling special category data are screened (e.g., BPSS/DBS) and trained in secure handling, data protection, incident reporting, and evidential integrity practices. Access follows least-privilege principles and is subject to MFA for privileged actions.

1.6.1 Data Protection and Encryption

- All data is encrypted in transit using TLS 1.2+ and at rest using AES-256, ensuring confidentiality and integrity across all storage and transfer points.
- Secure APIs and SFTP protocols are used for inbound and outbound data exchange, with strict authentication and authorisation controls.

1.6.2 Access Control

- Role-based access permissions enforced across all service components.
- Multi-factor authentication (MFA) required for administrative and privileged actions.

- Least-privilege principles applied to minimise risk.

1.6.3 Secure Development and Operations

- Development follows secure coding practices and is subject to vulnerability scanning and penetration testing.
- Change management processes ensure updates and patches are applied without service disruption.
- Continuous monitoring and alerting across infrastructure and application layers for threat detection and response.

1.6.4 Network and Infrastructure Security

- Defence-in-depth architecture with layered network security, including firewalls, intrusion detection/prevention systems, and segmentation.
- Regular security audits and compliance checks to maintain alignment with public sector requirements.

1.6.5 Compliance and Governance

- Full audit trails and immutable logging for all processing activities.
- Data residency guaranteed within UK jurisdiction, supporting UK GDPR and Data Protection Act 2018 compliance.
- Annual certification renewals and independent assessments to validate ongoing compliance.

1.7 Ancillary Services

Capita's ancillary services complement core scanning and digitisation, aligning with G-Cloud best practices and delivering innovative digital outcomes that drive efficiency, compliance, and transformation.

1.7.1 Document Migration and Integration

- Seamless transfer of documents, metadata, and records from legacy systems into Capita ECM or other platforms.
- Ensures business continuity, data integrity, and minimal disruption during onboarding or transformation.

1.7.2 Digital Mailroom Solutions

- Automated processing of inbound mail, converting physical documents into secure digital records.
- Integration with workflow systems for faster case handling and compliance reporting.

1.7.3 Records Management and Archiving

- Lifecycle management tools for retention policies, legal holds, and compliance audits.
- Supports BS 10008 standards for evidential weight and integrity of electronic information.

1.7.4 AI-Enhanced Data Capture and Mining

- Intelligent document processing using AI for classification, metadata extraction, and sentiment analysis.
- Enables automated triage, routing, and case creation for high-volume environments.

1.7.5 Agents and Agentic AI

- Agents: AI-driven virtual assistants designed to handle routine tasks such as email triage, appointment scheduling, and document routing.
- Agentic AI: Autonomous AI agents capable of orchestrating multi-step workflows, such as initiating document scanning, triggering compliance checks, and generating customer communications without manual intervention.

1.7.6 Customer Communications Management (CCM)

- Multi-channel communications (print, email, SMS) with AI-driven personalisation.
- GenAI for letter creation, automated approval checking, redaction, and sentiment-based escalation.

1.7.7 Digital Transformation, Integration and Automation

- Integration with enterprise systems for end-to-end process optimisation.
- AI-enabled workflows and Robotic Process Automation (RPA) to reduce manual intervention.

1.7.8 Data Analytics and Reporting

- Advanced analytics for operational insights and compliance dashboards.
- Supports predictive modelling and trend analysis for decision-making.

2 Service Features

The following features define the core capabilities of Capita's Scanning and Data Extraction service, ensuring secure, scalable, and intelligent processing of physical and digital content for public sector workflows.

- **AI-Enhanced Document Intelligence**
  Integrates multiple large language models within secure environments to optimise document processing and data extraction. Provides advanced classification, entity recognition, and contextual interpretation of unstructured content, reducing manual effort and improving accuracy. Generative AI supports summarisation and metadata generation, while OCR and language detection enhance processing. All AI workflows are configurable, auditable, and compliant with UK GDPR and responsible AI principles.

- **AI-Driven Operational Efficiency**
  Combines intelligent classification, sentiment analysis, and metadata capture for high-volume environments, enabling faster turnaround and improved data quality across public sector workflows.

- **Automated Data Extraction**
  Applies intelligent classification, indexing, and metadata tagging during digitisation workflows to ensure structured, searchable outputs ready for integration with downstream systems.

- **Secure Document Scanning**
  Converts physical documents into digital formats within UK-based, ISO-certified secure environments. Includes controlled access, monitored processes, and compliance with public sector security standards.

- **Electronic File Digitisation**
  Processes emails, structured, and unstructured electronic records into accessible digital assets, supporting multi-channel intake and consistent metadata application.

- **Secure Data Transfer**
  Enables inbound and outbound data exchange through secure protocols, including SFTP and API integration, ensuring confidentiality and integrity during transfer.

- **Encryption Standards**
  Protects data in transit using TLS and at rest using AES-256 encryption across all storage and transfer points, aligned with recognised security best practices.

- **Scalable Architecture**
  Built on modular, containerised components to support high-volume document ingestion and data extraction. Offers elastic capacity management and secure integration with enterprise systems via APIs and standard protocols.

- **Secure and Intelligent Processing Controls**
  Enforces role-based access permissions with multi-factor authentication for privileged actions. Provides comprehensive, centralised logging with immutable audit trails for compliance and operational assurance. AI-driven enhancements improve classification and reduce manual intervention, with all controls operating under UK GDPR and ISO frameworks.

- **Automated Backups and Disaster Recovery**
  Implements scheduled backups and tested recovery procedures to maintain business continuity and minimise disruption in the event of system failure.

- **Technical Scanning Specifications**
  - Resolution: 300–600 dpi; duplex capture supported
  - Colour modes: 24-bit colour and 8-bit greyscale
  - Formats: PDF/A-2b, TIFF G4, searchable PDF (OCR)

- Inputs: Paper sizes A5–A0, microfiche/film, bound volumes (by arrangement)
- Separation & indexing: Agreed page separation rules, file naming schema, and metadata index mapped at onboarding
- Quality Control: Sampling-based QC at agreed percentage per batch, with exception handling and re-work procedures

3 Service Benefits

The following benefits demonstrate the buyer-facing outcomes delivered by Capita's Scanning and Data Extraction service, each supported by a corresponding feature to ensure transparency and alignment with G-Cloud requirements.

- **Faster Document Processing (AI-Enhanced Document Intelligence):**
  AI-driven workflows accelerate document classification and extraction, significantly reducing turnaround times for high-volume environments. This ensures faster processing without manual bottlenecks, improving operational efficiency across public sector workflows.
- **Improved Data Accuracy (Automated Data Extraction):**
  Automated classification, indexing, and metadata tagging minimise human error and deliver consistent, reliable data capture. This accuracy supports compliance and enables better decision-making based on trustworthy information.
- **Enhanced Security and Compliance (Secure Document Scanning):**
  All scanning and digitisation activities occur within UK-based, ISO-certified secure environments. Combined with encryption and strict access controls, this ensures sensitive information is protected and meets public sector security standards.
- **Multi-Channel Capture Capability (Electronic File Digitisation):**
  The service handles both physical documents and electronic records, including emails and attachments, providing complete coverage for diverse inbound communication channels and reducing complexity for buyers.
- **Seamless System Integration (Secure Data Transfer):**
  Secure APIs and SFTP protocols enable smooth integration with existing public sector systems, ensuring data flows efficiently and securely between platforms without manual intervention.
- **Business Continuity Assurance (Automated Backups & Disaster Recovery):**
  Regular automated backups and tested disaster recovery procedures maintain service resilience and minimise disruption in the event of system failure, supporting continuity of critical operations.
- **Scalable to Demand (Scalable Architecture):**
  A modular, containerised architecture supports fluctuating document volumes and elastic capacity management, ensuring performance remains consistent even during peak demand periods.
- **Operational Transparency (Secure Processing Controls):**
  Centralised logging and immutable audit trails provide full visibility of all processing activities. This transparency supports compliance audits, governance requirements, and security investigations when needed.
- **Accessible Digital Records (Electronic File Digitisation):**
  Digitisation produces structured, searchable outputs that improve retrieval speed and accessibility for authorised users, enabling faster access to critical information across departments.
- **Supports Digital Transformation Goals (AI-Driven Operational Efficiency):**
  By reducing paper dependency and introducing intelligent automation, the service helps public sector organisations modernise workflows and align with government digital strategies.

4 Service Scope

The service subscription provides a complete managed solution for scanning, digitisation, and data extraction, designed for public sector compliance and operational efficiency. It includes the following elements:

Functionality

- Multi-channel document capture: physical scanning (bulk, day-forward, archive) and electronic file ingestion (emails, PDFs, structured/unstructured formats etc).
- Intelligent data extraction: OCR/ICR, classification, indexing, and metadata tagging.
- AI-enhanced processing: optional use of large language models for advanced interpretation and summarisation.
- Secure workflow automation: configurable business rules, approval hierarchies, and audit trails.
- Integration: APIs and secure file transfer (SFTP) for connectivity with ECM, case management, and line-of-business systems.
- Secure Physical Handling and Disposal: Physical originals are handled under approved procedures. Where destruction is requested or required, materials are processed through secure disposal with a certificate of destruction. Recyclable outputs are managed through recognised environmental channels.

Hosting

- Delivered as a managed private cloud service hosted in UK-based, ISO-certified environments.
- Data residency guaranteed within UK jurisdiction, aligned with UK GDPR and CCS security principles.
- No additional on-premise installation required; access provided via secure web interface or API.

Updates

- Continuous service improvements and feature updates included within the subscription.
- Security patches, compliance and updates applied proactively to maintain ISO 27001 and related standards.
- Enhancements rolled out without disruption, following controlled change management processes.

Support

- Standard support hours: Monday–Friday, 09:00–17:00 (UK time), excluding public holidays.
- Support channels: email, phone, and ticketing system; escalation paths defined in SLAs.
- Offboarding support: secure data extraction and transfer upon contract termination, ensuring buyer retains full access to digitised records.

Licence Model

- Subscription-based pricing aligned to G-Cloud requirements and the published pricing document.
- Tiered model based on transaction volumes and optional feature sets (e.g., AI processing).
- Service components, hosting, and updates included in the subscription fee.
- Additional services (e.g., bespoke integrations or accelerated onboarding) available under agreed rate card.

5 Disclaimer

All information contained in this document is provided in confidence for the sole purpose of adjudication of the document and shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without the prior permission in writing of Capita Group Plc and shall be held in safe custody. These obligations shall not apply to information that is published or becomes known legitimately from some source other than Capita Group Plc.