

Digital forensics case management

G-Cloud 15

Contents

Service overview	3
Features and benefits	5
Features	5
Benefits	5
Business continuity and disaster recovery plans	5
Onboarding and offboarding	6
Onboarding	6
Offboarding	6
Ways of working	6
Training.....	7
Quality assurance and performance testing	7
Security services.....	8
Ongoing support	8
SLA Incident response	9
Hosting managed services	9
Service constraints	10
Ordering and invoicing	10
Pricing	10
Industry standards	10
Contact details	11

Service overview

CDS provides a comprehensive Digital Forensics Case Management solution using the Appian platform. We provide implementation and ongoing support based on a range of options from off the shelf to accelerator modules that encompass the full suite of digital forensic activities including an integrated eQMS for ISO17025 compliance.

Appian provides:

- A SaaS platform that ensures performance, scalability, security and stability
- In-built, user interface-driven data modelling with a Data Fabric approach (entity relationships are understood by the application, allowing related data to be used in any screen or in any process)
- In-memory process data that enables efficient processing and reduces load time
- In-built, drag-and-drop-based process modelling, supporting orchestration of complex and parallel processes (incorporating user interactions via screens, logic gates, business rule interpretation and automation)
- 'Screen designer' interface providing drag-and-drop capability, with configuration to properties to enhance the experience
- Configuration-driven API access
- Configuration-driven RPA access
- A process mining module, with in-built visualisation of process operation and machine learning models that automatically suggest improvements.

Our Digital Forensics Product provides:

Data Management:

- Flexible data model
- Full auditing of access and CRUD operations
- Front end reference data management
- Automated and parameterised data retention.

Home pages for initial access points into the application providing a single view of activities, tasks and priorities:

Service requests and updates

- My Workspace for all personas in the Digital Forensics Unit
- Operations Management
- Exhibit Management
- Technical / Asset Management
- QMS Management.

Administration Services to efficiently orchestrate and manage activity

- Competency and availability based allocation with option to manage on an automated basis
- Individual and bulk re-allocation of tasks
- Parameter based intelligent prioritisation

- Exhibit handling and tracking including seal management
- Calendar based asset and resource availability
- Roles, groups and access policy management

Integrated eQMS module to reduce non-conformance and enable compliance with ISO17025

- Raise an issue on any process step or against any asset
- Triage and validate non-conformance
- Full non-conformance process with actions created and tracked
- DIP check process management
- Integrated issue log and process
- Integrated risk log and process
- Full document change request process with associated reading records
- Feedback / suggestions log and triage process

Integrated asset management module supports cost management and links to eQMS for compliance

- Hardware register with calibration process management
- Software register with licensing and version management
- Build register linked to hardware with full version contents and history
- Consumables register with usage predictions and re-order process
- Supplier register with full management information to understand usage across all assets and performance

User services to support and ensure your people use the system appropriately and efficiently

- Competency and competency management / validation process
- Fully searchable knowledge base with process step linkage and metadata tagging
- Contextual help available on each screen linked to the knowledge base

Full process control and orchestration including request, exhibit addition, DPN, advice, triage, strategy creation, extraction centrally and at kiosks, analysis, notes, communication and forensic reporting for:

- Computers / Hard Drives
- Mobile Devices
- Victim Identification
- On Scene services
- Digital services including CCTV and body mapping)
- Vehicle services

Full management information and analytics capabilities

- Power BI integration
- User and role based dashboards
- Self service reporting and analytics

AI powered insights including natural language based queries

We provide options to access this product as an off the shelf solution as well as providing professional services to support any level of customization you require. Our team has a deep understanding of the digital forensics landscape and can provide consultancy on both technical aspects of implementation as well as best practice to ensure ISO17025 compliance

Our consultancy services team are security cleared (BPSS, SC, NPPV2/3) by default and adept at working in closely governed, secure and regulatory environments.

Features and benefits

Features

- Request management, triage, prioritisation, allocation and exhibit management.
- Integrations to automate investigation, chain of command and exhibit details.
- Asset management for hardware, software, consumables and suppliers.
- Competency management and reading records.
- Process management for computers, mobiles, On Scene and Victim Identification.
- Process management for Vehicles, CCTV and digital services.
- Knowledge base for SOPs / Work Instructions linked to process steps.
- Full audit trail of access and change.
- Multiple templates and automated population of Streamlined Forensic Reports.
- Integrated QMS with non-conformance, issues, risks, feedback and change management.

Benefits

- Comprehensive, structured and guided end to end process management.
- Full visibility and management of all requests, progress and timings.
- Improved efficiency and resource utilisation.
- Integrations with core systems to remove re-keying of data.
- Competency and availability-based work allocation.
- Full chain of custody for exhibit management with barcode scanning.
- Simplified ISO17025 compliance and evidence provision for audits.
- Integrated QMS with validation steps to reduce non-conformance.
- System wide role-based access controls.
- MI provision including self-serve / custom reporting and AI powered insights.

Business continuity and disaster recovery plans

CDS is committed to minimising and managing its exposure to disruption to the business and the services provided to our customers. This encompasses robust systems and processes necessary to maintain continuity of service and operations.

CDS maintains a comprehensive Business Continuity and Disaster Recovery (BCDR) plan, certified to **ISO 23001**, that defines clear roles, responsibilities,

processes, and procedures for assessing and responding to disruptions to ensure continuity during disruptions. **Our plan is tested annually with lessons learned incorporated into plan improvements.**

Our Business Continuity Management System (BCMS) is underpinned by regular business impact assessments and threat and risk analyses, and annual tests to ensure all contingencies remain effective, current, and fit for purpose.

Onboarding and offboarding

Onboarding

CDS provides a tailored onboarding pathway, based on clients' individual requirements.

Onboarding is a collaborative process, through which we fully understand our clients' short-, medium- and long-term goals, and plan our service accordingly, to deliver best value and appropriate resourcing, governance, communication and planning.

Our multi-disciplinary agile teams will work with project stakeholders to understand the client and project needs and requirements.

We will define and capture ways of working, including definitions of 'ready' and 'done', and identify acceptance criteria for each sprint, underpinned by modern test practices and OKRs.

Offboarding

Upon starting the engagement, CDS will provide an exit plan for client approval. This will cover matters such as knowledge transfer and documentation, roll-off schedules, data and asset transfer, intellectual property and removal of access / permissions and return of devices / equipment.

Ownership of data contained in any solution belongs to and rests with the client; as the service is decommissioned, raw data will be transferred to the client. CDS is certified to ISO 27001 for data security and will always adhere to these standards – including data removal and destruction.

Ways of working

At CDS we apply agile principles across our projects, primarily using the SCRUM Agile methodology. We operate multi-disciplinary squads that combine domain expertise with technical excellence, delivering value early and iteratively through two-week sprints. Our approach is underpinned by the following core practices:

- **Daily standups:** A team call for 15 minutes each morning to track progress, surface blockers and ensure sprint goals are achieved.
- **Sprint planning:** Held at the start of each sprint to prioritise the work, align on objectives and ensure the team is fully prepared.
- **Sprint review:** At the end of the sprint, the team demonstrate to all stakeholders the deliverables achieved and present the sprint goal for the next sprint.

- **Sprint retrospective:** For each sprint the team will review what went well, identify areas of improvement and embed lessons learned to drive continuous improvement.

Additionally, we have an Agile mindset and culture at CDS, in which we apply:

- **User-centred design and customer-focus:** Through collaboration and partnership working we deliver outcomes that meet user needs.
- **Adaptability and flexibility:** Short feedback loops enable us to respond quickly to change, with teams empowered to pivot as required.
- **Continuous learning:** Retrospectives encourage open, honest feedback to continually improve ways of working and delivery effectiveness.
- **Partnership and teamwork:** We create a one-team culture with our clients and their supplier partners, working collectively towards shared project goals.

Training

As well as continual ‘on the job’ knowledge transfer to upskill client teams, CDS can provide formal, comprehensive training for administrators and users prior to handover and go live designed to support successful change management, ensure smooth implementation and embed solutions that are integral to business operations. Our training also builds internal technical capability, empowering teams to become self-sufficient and reduce the long-term cost of change.

In most cases, we adopt a ‘train-the-trainer’ model, delivered through a blend of on-site and remote sessions. This is supported by comprehensive training materials and easy-to-follow digital end-user guides, written for non-technical audiences and compliant with WCAG 2.2 accessibility guidelines.

Quality assurance and performance testing

CDS applies rigorous testing as part of our Quality Assurance process (ISO9001) to ensure we maintain quality across our deliverables and that outcomes are fit for purpose and fulfil functional and performance requirements.

Our testing capability is led by ISTQB (International Software Testing Qualifications Board) qualified testing experts with all the skills and expertise to quality assure AI, technology & cloud services.

We use a flexible, agile testing approach utilising tools and techniques tailored to each client’s context to ensure solutions meet business objectives and success criteria.

We adopt an automation-first approach, embedding high-quality automated checks into robust CI/CD pipelines to ensure quality is treated as a first-class citizen throughout the deployment process.

Our testing services include:

- Test strategy
- Test planning

- Automated test frameworks
- Testing, defect management and reporting
- Support of customer UAT
- Security (perimeter/application) testing / DevSecOps
- Performance and stress testing.

Security services

CDS holds certifications to international standards - Cyber Essentials Plus and ISO27001 Information Security, encompassing physical security, personnel security, storage, electronic data handling and secure destruction.

We embed 'secure-by-design' principles in our standard service design approach, aligned with security best practises and in addition we provide expert security consultancy.

CDS works closely with National Cyber Security Centre CHECK-accredited providers to conduct IT Health Checks (ITHC)/penetration testing in line with best practice.

CDS staff are BPSS cleared as a minimum. We can deploy SC, NPPV cleared teams and staff with DV clearance, if required.

Ongoing support

Our service model is designed to provide comprehensive, proactive support that operates to

ISO20000:2018 Service Management and ITIL best practices, covering the full-service management lifecycle.

We deliver a fully managed service that encompasses application support, platform maintenance, incident management, problem management, change management, supplier management, and out-of-hours support for major incidents. This approach ensures that business-critical systems remain operational and performant whilst maximising customer value through continuous service improvement.

All CDS Service Delivery team are ITIL-certified.

We offer three service levels (Bronze, Silver and Gold) each providing:

- Online Service Desk Portal available 24x7 for logging and tracking incidents and requests.
- Telephone support via a dedicated helpline available from 9am to 5pm Monday – Friday (excluding English Bank Holidays).
- Highly skilled service desk team who manage and resolve incidents and requests in accordance with the agreed SLA.
- Ongoing maintenance including application of security patches.
- Structured change management to ensure updates are properly assessed, approved and implemented.
- Monthly performance report to provide visibility of service levels and operational metrics.

Support and maintenance contracts stipulate a minimum level of support provision per month, appropriate to the size and complexity of the service, aligned to the preferred service support tier. Additional time is chargeable at the day rates listed on the rate card.

SLA Incident response

Service	Bronze	Silver	Gold
Incident response			
P1 - To be called in	15 minutes	15 minutes	15 minutes
P2	1 hour	1 hour	1 hour
P3	1 hour	1 hour	1 hour
P4	4 hours	4 hours	1 hour
P5	1 working day	1 working day	1 hour
P6	1 working day	1 working day	1 hour
Target incident resolution - core hours			
P1	8 hours	6 hours	4 hours
P2	15 hours	11 hours	8 hours
P3	5 working days	3 working days	1 working day
P4	7 working days	5 working days	3 working days
P5	N/A	14 working days	10 working days
P6	N/A	N/A	N/A
Major Incident Report	N/A	10 working days	5 working days

Hosting managed services

CDS provides a range of consultancy and management services for design, implementation and management of application infrastructure, including:

- Technical architecture and implementation
- Infrastructure management and maintenance including:
- Critical security patches
- OS (operating system) patches: testing and deployment
- Application and platform availability
- Anti-virus & Malware updates
- Obsolescence management
- Proactive monitoring and alerting of Infrastructure & solution performance and function.

Service constraints

Attainable service levels will be dependent upon the service performance of cloud suppliers within the service chain. Maintenance windows may apply, and clients should refer to the SLA for the specific service in use.

Ordering and invoicing

We recommend contacting CDS before placing an order via G Cloud 15, to confirm and agree scope, scale, SLAs, KPIs, outcomes, etc. We will be pleased to support clients to define statements of work that reflect their requirements.

Invoices are issued monthly in arrears, with payment terms of 30 days.

Pricing

Timescales and costs vary, depending on several factors; we recommend a preliminary review to provide a firm cost.

Please refer to our pricing document and rate card.

Industry standards

CDS delivers all its services to internationally recognised standards. CDS is accredited to the following standards:

- ISO 9001 Quality Management System.
- ISO 27001 Information Security Management.
- ISO 20000 IT Service Management and IASME certified.
- ISO 14001 Environmental Management.
- BSI 1008 Electronic Information.
- ISO 22301 Security and Resilience (Business Continuity).
- ISO 45001 Health and Safety Management.
- ISO 10008 Evidential Weight and Legal Admissibility of Electronic Information.
- ISO 50001 Energy Management Standard.
- Cyber Essentials Plus.
- IASME certified.
- ITIL compliant service desk.
- PlanetMark Sustainability.

We comply with the Data Protection Act 2018 and UK GDPR regulations.

Contact details

Matt Johnson,
Head of Public Sector
CDS, Yorkshire House, Greek Street, Leeds, LS1 5SH
Email: bidteam@cds.co.uk
Telephone: 07939 866831
Website: www.cds.co.uk