

Cloudflare Catalyst Implementation & migration services

G-Cloud 15

Contents

Service overview	4
About CDS.....	4
Features and benefits	4
Features.....	4
Benefits	5
Service scope	5
New Client Implementation	5
Migration Services.....	5
Service Tiers & Timeline	5
Complexity Assessment Framework	6
Low Complexity.....	6
Medium Complexity.....	6
High Complexity	7
Implementation Methodology - The 5 Ds	9
Phase 1: Discover	9
Phase 2: Define.....	9
Phase 3: Design.....	10
Phase 4: Deliver.....	10
Phase 5: Develop.....	11
Roles & Responsibilities	11
Deliverables	11
Service Level Commitments	12
Assumptions & Dependencies	12
Out of Scope	12
Business continuity and disaster recovery plans	13
Onboarding and offboarding	13
Onboarding	13
Offboarding	13
Ways of working	Error! Bookmark not defined.
Training.....	Error! Bookmark not defined.
Quality assurance and performance testing	13
Security services.....	14

Service constraints	14
Ordering and invoicing	14
Pricing	15
Industry standards	15
Contact details	15

Service Overview

CDS provides comprehensive Cloudflare implementation and migration services designed to help organisations seamlessly transition to or optimise their use of the Cloudflare platform. Our services encompass the complete lifecycle from initial assessment and planning through to deployment, testing, and post-implementation support.

Whether you're implementing Cloudflare for the first time or migrating from a competitor service, our experienced team ensures a smooth transition with minimal disruption to your operations.

About CDS

CDS is Cloudflare's first Authorised Service Delivery Partner (ASDP) in EMEA, and one of their most certified.

Our Cloudflare Catalyst onboarding services offers expert consultancy and hands-on support, enabling organisations to fully harness Cloudflare's global network for enhanced security, performance, and scalability.

We've deployed and managed Cloudflare for multiple organisations across government, finance, retail, entertainment, media, and professional services including:

- **National Police Chiefs' Council** - Single Online Home digital policing platform used by 41 out of 43 police forces (available to 90+% of citizens in England and Wales) to report non-emergency crime
- **David Lloyd** - high profile national chain of health clubs with 730,000 members across 133 clubs and in nine countries.
- **National Rail Enquiries** - gateway to Britain's National Rail network, receiving an average of 2.5 million visitors per day using the website's Journey Planner.

Features and Benefits

Features

1. Structured 5D methodology: Discover, Define, Design, Deliver, Develop phases
 2. Terraform Infrastructure as Code deployment for consistent configuration management
 3. Complexity assessment across Customer, Project, Solution and Delivery factors
 4. Expert Cloudflare architects with cross-industry best practice experience
 5. Comprehensive security configuration including WAF, Zero Trust and DDoS
 6. Performance optimisation with caching, Workers and traffic management setup
 7. 30-day post-deployment optimisation and stabilisation support included
 8. Flexible timelines: 4 weeks low, 8 weeks medium, 12 weeks high complexity.
-

Benefits

1. Minimised business disruption through structured phased implementation approach
2. Future-proof architecture designed for scalability and long-term growth
3. Reduced security risk with comprehensive configuration testing
4. Faster time to value with experienced specialists and proven methodologies
5. Knowledge transfer ensures internal teams can manage ongoing operations
6. Clear accountability with defined roles, deliverables and milestone tracking
7. Confidence through comprehensive testing before production cutover
8. Seamless migration from competitor platforms with minimal downtime

Service Scope

New Client Implementation

For organisations new to Cloudflare, our service includes:

- Current infrastructure assessment and requirements gathering
- Cloudflare product selection and architecture design
- DNS configuration and zone setup
- SSL/TLS certificate provisioning and configuration
- Security rules, firewall rules, and WAF configuration
- Performance optimisation including caching rules and page rules
- Load balancing and traffic management setup (if applicable)
- Integration with existing systems and workflows
- Testing and validation across all configured services
- Knowledge transfer and documentation.

Migration Services

For organisations migrating from competitor platforms, our service includes:

- Comprehensive audit of current CDN/security provider configuration
- Gap analysis and feature mapping from existing platform to Cloudflare
- Migration strategy and detailed cutover plan
- Configuration replication and rule translation
- Parallel testing environment setup
- Staged or full cutover execution with rollback procedures
- Post-migration validation and performance comparison
- Optimisation recommendations based on Cloudflare capabilities
- Decommissioning support for legacy platform.

Service Tiers & Timeline

Project complexity is assessed across four key dimensions: Customer factors, Project factors, Solution factors, and Delivery factors. This assessment determines the appropriate service tier and timeline for your implementation.

Complexity Assessment Framework

We evaluate projects based on the following criteria:

Customer Considerations:

Industry sector and regulatory requirements, organisational structure and governance, number of stakeholders, technology maturity and readiness, current security posture

Project Considerations:

Stakeholder availability and geographic distribution, project timeline and dependencies, governance and change management processes, non-functional requirements, delivery methodology requirements

Solution Considerations:

Greenfield vs migration scenario, existing documentation quality, number and variety of applications and user groups, policy and configuration volume, technology stack alignment, required integrations

Delivery Considerations:

Rollout methodology (big-bang, phased, POC), handover vs managed service approach, documentation and training requirements, monitoring and logging needs, infrastructure as code requirements, testing scope and expectations

Application Services

Low Complexity

Duration: 3 - 4 weeks

Characteristics:

- Straightforward organisational structure with clear decision-making
- Limited compliance requirements and modern technology stack
- Single or few locations, minimal external dependencies
- Standard Cloudflare features with minimal customisation
- Big bang deployment with standard documentation.

Typical Scope:

- Single domain or small number of subdomains
- Standard SSL/TLS configuration
- Basic security rules and firewall configuration
- Standard caching policies
- Limited compliance requirements.

Medium Complexity

Duration: 5.5 - 7.5 weeks

Characteristics:

- Multi-departmental stakeholders with some governance layers
- Industry-specific compliance and semi-modern technology environment
- Multiple locations with some external supplier dependencies
- Advanced Cloudflare features including Workers and custom configurations
- Phased or segmented rollout with comprehensive documentation.

Typical Scope:

- Multiple domains or complex subdomain structures
- Advanced security configurations (WAF, rate limiting, bot management)
- Custom page rules and caching strategies
- Load balancing across multiple origins
- Limited integrations.

High Complexity

Duration: 12 - 20 weeks

Characteristics:

- Complex governance with multiple approval layers and group structures
- Heavily regulated industry with critical service requirements
- Multi-location, multi-timezone operations with numerous dependencies
- Extensive customisation, sophisticated integrations, and potential technology transformation
- POC and iterative phased rollout with comprehensive testing and managed service transition.

Typical Scope:

- Enterprise-scale deployments with numerous domains
- Complex multi-region architectures
- Advanced Workers applications and custom logic
- Complex migration from multiple legacy providers
- Extensive API integrations and automation
- Custom development and advanced configurations
- Compliance requirements (PCI-DSS, HIPAA, etc.).

Note: The final complexity assessment is determined during the Discover and Define phases through consultation with your team and technical assessment of your environment.

Cloudflare One

Cloudflare One implementation can include Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG/SSE), and Secure Access Service Edge (SASE) solutions covering Zero Trust Access, Gateway, WARP, Tunnel, and related security features.

Low Complexity

Duration: 5 - 11 weeks

Characteristics:

- Single site or limited user base deployment
- Straightforward identity provider integration
- Basic Zero Trust policies and access controls
- Standard Gateway filtering and security policies
- Limited number of applications or resources to protect
- Simple organisational structure with clear approval processes.

Medium Complexity

Duration: 10 - 22 weeks

Characteristics:

- Multi-site deployment with regional considerations
- Multiple identity providers or complex user directory structures
- Advanced Zero Trust policies with contextual access controls
- Custom Gateway policies with DLP and tenant controls
- Moderate application portfolio with mixed access requirements
- Multi-departmental stakeholders with governance requirements.

High Complexity

Duration: 19 - 47 weeks

Characteristics:

- Global deployment across multiple regions and time zones
- Complex identity and access management architecture
- Comprehensive SASE implementation with full security stack
- Sophisticated Zero Trust architecture with device posture and risk-based access
- Large-scale user base with diverse access requirements
- Extensive integrations with existing security tools and SIEM platforms
- Heavily regulated environment with strict compliance requirements
- Phased rollout with extensive testing and pilot programs.

Enterprise Implementations

For enterprise-scale projects with notable size, breadth, and variability of scope and complexity, a bespoke proposal will be required. Such projects will typically use high complexity scope as a foundation to tailor and likely build upon. Contact CDS to discuss your enterprise requirements.

Note: The final complexity assessment and accurate pricing are determined during the Discover and Define phases through consultation with your team and technical assessment of your environment. Costs shown are estimates and may vary based on specific requirements.

Implementation Methodology - The 5 Ds

Our implementation approach follows a structured five-phase methodology designed to ensure comprehensive understanding, effective solution design, and successful deployment of your Cloudflare environment.

Phase 1: Discover

Objectives:

- **Strategic & Commercial Context:** Understanding your current state, reason for change, commercial and strategic objectives, success criteria/KPIs, and desired future state
- **Operational Context:** Identifying operational objectives, user groups and personas
- **Risk Assessment:** Reviewing compliance requirements, current security risks and incidents
- **Technical Context:** Defining technical objectives, application/network discovery, architecture gap analysis, and documentation/code review
- **Ways of Working:** Establishing timelines, roles and responsibilities, skills assessment, barriers and enablers, documentation and reporting requirements

Deliverables:

- Facilitated workshops with client and relevant stakeholders
- Desk research and review of current configuration in existing solution
- Documentation and codebase review
- Audit of current implementation
- Preliminary security reconnaissance

Phase 2: Define

Objectives:

- Collate gathered information and extract key insights most pertinent to understanding context and importance of requirements
- Document processes and topics of discovery
- Provide summary and prioritisation of key findings and objectives

- Confirm understanding with client.

Deliverables:

- Comprehensive report documenting findings and context
- Playback session with client
- Confirmed understanding and agreement on requirements

Phase 3: Design

Objectives:

- Design and propose a solution that efficiently and effectively solves the immediate use case
- Ensure solution contributes to wider technology, security, operational, commercial and strategic objectives
- Receive sign-off to invest and progress.

Deliverables:

- **Solution Design:** High Level Design (HLD) document, Low Level Design (LLD) document if required, Terraform baselines configured/aligned
- **Delivery Planning:** Scope of Works and delivery plan including testing and cutover plan, RAID log if applicable
- **Commercial Proposal:** Business case and commercial proposal covering licenses and services

Phase 4: Deliver

Objectives:

- Deliver to agreed objectives and KPIs of the client, their users and relevant third parties
- Meet any regulatory requirements
- Ensure client is ready and able to manage and maximise value of the solution.

Deliverables:

- **Configure:** Execute Terraform baseline test scripts, configure logging and SIEM integrations, create reports and dashboards
- **Deploy:** Infrastructure as Code via Terraform (unless feature restrictions or client preference requires manual deployment)
- **Test:** Confirm test resource dependencies, peer-to-peer configuration validation against HLD/LLD, senior review and client sign-off, execute required tests and confirm success criteria, penetration testing if required, client UAT testing, final validation and change freeze
- **Cutover:** Change Approval Board collaboration according to plan and ITSM approach.

Phase 5: Develop

Objectives:

- Enable timely access to expert resources for ongoing management, optimisation and incident response
- Continuously improve and evolve the solution.

Deliverables:

- **Optimisation:** 1-month post-deployment monitoring and optimisation (included)
- **Professional Services:** Ongoing or periodic management, optimisation and consultancy (priced on demand)
- **Managed Services:** 24/7 SLA-backed incident response (priced on demand).

Roles & Responsibilities

CDS Responsibilities

- Project management and coordination
- Technical implementation and configuration
- Testing and validation
- Documentation and knowledge transfer
- Issue resolution during implementation
- Best practice recommendations.

Client Responsibilities

- Timely provision of required information and access
- Cloudflare account and licensing procurement
- DNS management authority and access
- Designated technical and business stakeholders
- User acceptance testing participation
- Approval of key milestones and go-live decisions
- Internal communication and change management.

Deliverables

- Current state assessment report (migration projects)
- Architecture design document
- Implementation plan and timeline
- Configured Cloudflare environment per specifications
- Security configuration documentation
- Performance optimisation report
- Testing results and validation reports
- Runbook and operational documentation
- Knowledge transfer sessions
- Post-implementation recommendations.

Service Level Commitments

Activity	Timescales
Project Kick-off	Within x business days of contract execution
Response Times: Critical issues during implementation	4 business hours; Standard queries - 1 business day
Status Reporting:	Weekly progress updates and bi-weekly stakeholder meetings
Post-Implementation Support:	30 days of stabilisation support included following go-live

Assumptions & Dependencies

Assumptions

- Client has appropriate Cloudflare subscription for required features
- Client provides timely access to necessary systems and information
- Project scope is clearly defined and documented
- Client has authority to make DNS changes
- Testing environments are available as needed.

Dependencies

- Client stakeholder availability for decisions and approvals
- Access to existing platform configurations (for migrations)
- Coordination with third-party vendors if applicable
- Maintenance windows for cutover activities
- SSL certificates and domain verification materials.

Out of Scope

The following items are not included in this service definition unless explicitly agreed:

- Ongoing managed services or 24/7 support (available separately)
- Application code modifications or origin server optimisation
- Content creation or website design changes
- Training beyond the included knowledge transfer sessions
- Cloudflare licensing costs
- Third-party software licenses or tools
- Infrastructure changes outside of Cloudflare configuration

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.

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.

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.

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