

Cloudflare Catalyst Audit

G-Cloud 15

Contents

Service overview	4
About CDS.....	4
Features and benefits	4
Features.....	4
Benefits	4
Service scope	5
Audit coverage areas	5
What we assess	5
Audit methodology	6
Phase 1: Discover	6
Phase 2: Define.....	6
Timeline & engagement.....	7
Deliverables	7
Comprehensive Audit Report	7
Playback Session.....	7
Optional: Remediation Proposal.....	7
Roles & Responsibilities	8
CDS Responsibilities.....	8
Client Responsibilities	8
Prerequisites.....	8
Ideal candidates for audit service	8
Out of scope	8
Next steps after audit.....	9
Business continuity and disaster recovery plans	10
Onboarding and offboarding	10
Onboarding	10
Offboarding	10
Ways of working	10
Training.....	11
Quality assurance and performance testing	11
Security services.....	12
Service constraints	12

Ordering and invoicing	12
Pricing	12
Industry standards	13
Contact details	13

Service overview

CDS provides comprehensive Cloudflare Audit services designed to assess your current Cloudflare implementation against industry best practices, identify security risks and performance optimisation opportunities, and provide clear recommendations for improvement.

Our expert audit service helps organisations understand how well their Cloudflare configuration aligns with best practices, uncover potential security vulnerabilities, and identify opportunities to maximise the value of their Cloudflare investment.

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. Fixed price comprehensive audit covering 20 critical configuration areas.
2. Expert architect review with read-only platform access analysis.
3. Two-phase Discover and Define methodology for thorough assessment.
4. Detailed audit report with prioritised actionable recommendations.
5. Security, performance, governance and operational effectiveness evaluation.
6. Best practice alignment assessment against Cloudflare and industry standards.
7. Interactive playback session with stakeholders for findings discussion.
8. Fast turnaround: 1-2 weeks from kick-off to report delivery.

Benefits

1. Identify security vulnerabilities before they can be exploited.
2. Uncover performance optimisation opportunities to improve user experience.

3. Ensure configuration follows industry standards and best practices.
4. Minimal client time commitment: approximately 5-6 hours total.
5. Independent expert assessment from experienced Cloudflare specialists.
6. Clear prioritised roadmap guides improvement efforts effectively.
7. Cost-effective way to validate and optimise existing Cloudflare investment.
8. Foundation for informed decisions on expansion or enhancement initiatives.

Service scope

Our Cloudflare Audit service provides a thorough evaluation of your Cloudflare environment across key operational, security, and performance domains. The audit follows our proven Discover and Define methodology to ensure comprehensive coverage and actionable insights.

Audit coverage areas

Security & Access

- Role-Based Access Control
- DNS Security
- WAF Rules
- Bot Management
- Rate Limiting
- Zero Trust Access Policies
- Secure Tunnels
- Network Security
- Certificate Management.

Performance & Configuration

- Caching Configuration
- Performance Settings
- Traffic Routing
- Workers & Scripts
- Page/Transform Rules
- Zone Configuration Consistency.

Governance & Standards

- Naming Conventions Review
- Architecture Alignment
- Configuration Consistency
- Best Practice Compliance.

Monitoring & Operations

- Audit Logs Review
- Firewall Events Review
- Logging Strategy
- Operational Effectiveness.

What we assess

Alignment with Best Practice: How well your configuration follows Cloudflare and industry best practices.

Security Risks: Potential vulnerabilities or misconfigurations that could impact security and performance.

Optimisation Opportunities: Areas where configuration improvements could enhance performance, reduce costs, or improve user experience.

Architectural Consistency: Alignment between your current state and intended architecture.

Operational Readiness: Effectiveness of logging, monitoring, and incident response capabilities.

Audit methodology

Our audit follows a structured two-phase approach designed to thoroughly understand your environment and provide actionable recommendations.

Phase 1: Discover

Stage: Understand context and need

Objectives:

- Understand use case and business objectives
- Define technical objectives and review wider environment
- Conduct resource and skills assessment.

Activities:

- Teams call with relevant client-side stakeholders (maximum 2 hours)
- Understand business context, current challenges, and success criteria.

Stage: Review existing Cloudflare configuration

Objectives:

- Assess alignment with best practice
- Identify risks to security and/or performance
- Uncover opportunities for improvements.

Activities:

- Read-only access review of Cloudflare platform by expert architect
- Comprehensive evaluation across all 20 audit coverage areas
- Documentation and codebase review where available
- Configuration assessment against industry standards.

Phase 2: Define

Stage: Make recommendations

Objectives:

- Clarify what changes should be made and why they are important.
- Identify if additional Cloudflare products would be beneficial.
- Can include proposal for required time, investment and next steps.

Deliverables:

- Collate findings and compile comprehensive audit report (PowerPoint/PDF format).
- Playback call with client stakeholders (maximum 2 hours).
- Clear prioritisation of recommendations.
- Proposed remediation roadmap (if requested).

Timeline & engagement

Total Duration: Typically, 1-2 weeks from kick-off to final report delivery.

Client Time Commitment:

Activity	Time
Initial discovery call:	Maximum 2 hours
Provision of read-only Cloudflare access	1 hour
Final playback session	Maximum 2 hours
Total client engagement time:	Approximately 5-6 hours

Flexible Scheduling: We work around your team's availability to minimise disruption to operations.

Deliverables

Comprehensive Audit Report

Professional report (PowerPoint or PDF format) including:

- Executive summary of key findings
- Detailed assessment across all 20 coverage areas
- Security risks and vulnerabilities identified
- Performance optimisation opportunities
- Best practice alignment scoring
- Prioritised recommendations with rationale
- Potential benefits of recommended changes
- Suggested Cloudflare products or features for consideration.

Playback Session

Interactive presentation and discussion of findings with your stakeholders, including Q&A and clarification of recommendations.

Optional: Remediation Proposal

If requested, we can provide a detailed proposal outlining the time, investment, and approach required to implement recommended changes.

Roles & Responsibilities

CDS Responsibilities

- Conduct discovery workshop and stakeholder interviews
- Perform comprehensive technical audit of Cloudflare environment
- Analyse configuration against best practices and industry standards
- Identify security risks, performance issues, and optimisation opportunities
- Compile detailed audit report with prioritised recommendations
- Deliver playback session with findings and recommendations
- Provide clarification and answer questions on findings.

Client Responsibilities

- Participate in initial discovery call (up to 2 hours)
- Provide read-only access to Cloudflare environment
- Share relevant documentation (architecture diagrams, runbooks, etc.)
- Designate key stakeholders for playback session
- Participate in final playback session (up to 2 hours)
- Provide context on business objectives and constraints.

Prerequisites

- Active Cloudflare account with existing configuration
- Ability to provide read-only access to Cloudflare environment
- Availability of key stakeholders for discovery and playback sessions
- Basic documentation of intended architecture (helpful but not required).

Ideal candidates for audit service

This service is particularly valuable for organisations that:

- Have inherited Cloudflare configurations from previous teams or vendors
- Have made incremental changes over time without comprehensive review
- Are experiencing performance issues or security concerns
- Want to validate their current configuration before scaling
- Are considering expanding their use of Cloudflare products
- Need to demonstrate compliance with security standards
- Are planning a major architecture or infrastructure change
- Want an independent expert assessment of their Cloudflare investment.

Out of scope

The following items are not included in the standard audit service:

- Implementation of recommended changes (available as follow-on service)
- Ongoing monitoring or managed services
- Penetration testing or active security assessments
- Application code review or optimisation

- Origin server configuration or optimisation
- Training or knowledge transfer sessions beyond the playback call
- Architecture design documentation (HLD/LLD) unless explicitly requested.

Next steps after audit

Following completion of the audit, clients typically pursue one or more of these paths:

- **Self-Implementation**
 - Use the audit findings and recommendations to guide internal implementation of improvements.
- **Engagement for Remediation**
 - Partner with CDS to implement recommended changes through our professional services.
- **Managed Services**
 - Transition to ongoing managed services for continuous optimisation and 24/7 support.
- **Periodic Re-Assessment**
 - Schedule follow-up audits to track improvements and identify new optimisation opportunities.

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.

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