Information assurance and security

Information for digital transition lead, technical support

Updated: November 6 2013

GOV.UK has been developed by the Government Digital Service (GDS) as a platform based on open source technologies. The information is published by and on behalf of UK ministerial departments, other departments and agencies of HM government.

The underlying architecture of GOV.UK

A content delivery network (CDN) supports low latency page access and high availability.

Web application software provides:
- web pages and other content assets (such as PDF documents)
- editorial and administrative functions that allow for distributed management of web publishing
- administration of users authorised to publish content

Data and search services are built on top of widely deployed open-source infrastructure, such as MySQL, MongoDB and ElasticSearch.

GOV.UK is hosted on cloud (Infrastructure as a Service) based servers using on the open
source Linux operating system. All of the origin servers are located within UK datacenters. CDN cache nodes are global.

The application components that comprise GOV.UK and the infrastructure that supports them are accredited in line with HMG Infosec Standard No 1 and regularly tested for security and resilience.

Assurance and accreditation
The information assurance process has addressed elements of the GOV.UK platform in different ways, as follows:

- **hosting**: GOV.UK is hosted on a GCloud service that has been accredited by Pan Government Accreditors
- **GOV.UK technical solution and supporting GDS operations**: this has been through a full HMG accreditation process and has been formally accredited (further details below)
- **Content Delivery Network (CDN)**: GOV.UK uses a CDN to deliver its content across the globe, which has been subject to a thorough assurance process (further details below)
- **development and operational processes**: in addition to the standard review of operational procedures carried out as part of the baseline control set review, the development and operational procedures are under review with the accreditor to confirm they are fit for purpose and producing quality outcomes.

GOV.UK Business Impact Levels
For the public web site: Confidentiality = 1, Integrity = 4, Availability = 4
For the publishing service: Confidentiality = 2, Integrity = 3, Availability = 2

CESG - the national technical authority for information assurance
CESG has provided ongoing support during the design and build of GOV.UK. It has provided guidance as well as carrying out technical reviews of the GOV.UK architecture.

Method of accreditation
The hosting platform on which GOV.UK sits has been accredited by the Pan Government Accreditors. The GOV.UK technical solution and supporting GDS operations have been through a full HMG accreditation process including Baseline Control Set review, IS1 & IS2 formal risk assessment and a comprehensive IT Health Check (ITHC) programme. A Risk Management and Accreditation Documentation Set (RMADS) has been produced and the residual risks / risk treatment plan are actively managed and will continue to be throughout the life of the service.

Scope of IT health check programme
The IT health check programme has covered application vulnerability testing, server build reviews, firewall reviews and DDoS tests. The testing was carried out in several stages throughout the build process leading up to go live and an ongoing programme of ITHC testing will
continue throughout the life of the service. We used CHECK test teams to carry out this work.

**Method to assure the GOV.UK CDN**
Fastly is the provider of the Content Delivery Network used by GOV.UK. As the Fastly service is not yet a GCloud service it does not have PGA accreditation. As a result, an assurance activity was carried out by a CLAS consultant and GDS Accradiator.

The assurance activity relied on the following factors and activities:
- a Snapshot IS1 risk assessment
- IT Health Check testing of the Fastly infrastructure and service
- a review of Fastly’s ISMS

**Risk owner**
The Cabinet Office owns the risk for GOV.UK.

GDS supports the GOV.UK platform. The platform is supported by a cross-functional group consisting of infrastructure specialists and software developers with a defined escalation process to the GDS technical architect team.

**Managing ongoing information assurance for GOV.UK**
Various activities are carried out for ongoing management of GOV.UK Information Assurance.

These include:
- active management of the risk treatment plan
- an ongoing programme of IT health checks on the platform, including i) regular quarterly IT health checks and ii) security impact assessment of change to determine whether an ITHC is required for any particular change being made to the platform that falls outside the quarterly checks
- annual review of the GOV.UK platform accreditation status
- security impact assessments to determine whether a change to the GOV.UK platform necessitates either a simple notification of change or a re-run of the IS1 and IS2 risk assessment and associated RMADS updates.

**Support levels**
The entire GOV.UK platform is supported 24x7 with a 15-minute service level agreement between GDS and our IaaS partners. If a critical alert is raised (inside or outside of business hours) the alert will be acknowledged within 15 minutes and preliminary investigation will begin.

GOV.UK has a sophisticated monitoring system based on open source tools, which constantly validates the availability and performance of the platform. Supporting tools provide extensive instrumentation of application components and aggregation of machine data, such as application logging.
GDS product teams provide application support with an escalation process to the GDS technical architecture team.

**Level of resilience**
The GOV.UK publishing platform has multiple layers of resilience built into it. These underwrite the availability of the system. The CDN allows [GOV.UK](http://transition.blog.gov.uk) to leverage servers located in countries around the world. This provides a significant degree of resilience. All GOV.UK application and data services are placed in fault-tolerant clusters. These include:

- web application servers
- search applications servers
- database services
- document store servers

GOV.UK is hosted on a virtualised platform that provides high availability to mitigate the possibility of hardware failure at the machine virtualisation (hypervisor) layer. All IaaS cloud hosting that supports GOV.UK is within a high availability, fault tolerant networking environment with multiple redundant connections to multiple ISPs.

**Disaster recovery**
The GOV.UK publishing platform support group has planned for recovery from a variety of disaster events. The support group performs recovery drills and keeps an up-to-date documentation set up.

The GOV.UK CDN provides a massively redundant and geographically distributed static mirror of the GOV.UK site. This static mirror can be switched for the GOV.UK site at very short notice. GOV.UK has a redundant geographically separate data centre so that the entire platform can be failed over to an alternate location within hours. GOV.UK data is backed up daily to both onsite and offsite storage arrays.

**Stay in the loop**
We’ll be keeping our dedicated blog updated throughout the transition - read more at [http://transition.blog.gov.uk](http://transition.blog.gov.uk)