Cabinet Office

Competition and Markets Authority (CMA) Screening for Cartels tool
Government Digital Service (GDS) Statement of Assurance

Audience

This document is intended for those who need to understand the Government Digital Service's ("GDS") approach to information assurance and information risk management for the Cartel Screening Tool created by the Competition and Markets Authority (CMA).

Background

The CMA requested that GDS provide technical guidance; which was supplied by the GDS architecture team. GDS were also asked to undertake an information assurance activity for the product to verify that it is fit for purpose to be used on an HMG hosted endpoint and in turn to facilitate easier take up of the product across HMG.

The risk assessment has identified a set of risks for consideration by departments wishing to use the tool.

Our approach

The approach we have taken is aligned to the guidance provided by the National Cyber Security Centre (NCSC) on GOV.UK.

The formal risk assessment has included:

- a formal risk assessment using a methodology based on ISO 27005:2011
- CHECK-based IT Health Check testing
- the creation of a residual risk statement and risk treatment plan
- Review of the risk assessment and risk treatment plan by the Cabinet Office SIRO Working Group, which is responsible for oversight of information risk management across the Cabinet Office.

The risks identified are subject to a risk treatment plan and the residual risks should be actively managed throughout the life of the service.

IT Health Check Testing

The IT Health Check programme has covered:

- application vulnerability testing.

GDS recommends that retesting of the tool be carried out in the event that significant change is made to the tool. We used CHECK test teams to carry out this work.

Risk Acceptance[1]

The risks identified are set out for acceptance by the CMA SIRO and by the relevant parties in the department's who use this tool.

[1] This has parallels with Accreditation models but is in alignment with Government Security Secretariat policy.

Ongoing Information Risk Management

The ongoing management of information assurance should include:

- the active management of the risk treatment plan by CMA
- IT Health Checks (annual or on major change)
- security impact assessments to determine whether a change to the service necessitates:
    - either a re-run of the risk assessment or
    - requires an ITHC test.

Frequently Asked Questions

1. **What is the approach to Risk Management?**

Response: The approach taken to risk management follows recognised industry good practice for risk assessment and management, as contained within ISO 27005:2011 supplemented by reference to NCSC standards and guidance documentation. Risks are identified by completion of the review of the solution design, intended operation and ITHC testing activity and are recorded and managed by use of a Risk Table and Risk Treatment Plan.

2. **Which Security Classification applies?**

Response: Information within the tool is deemed to be commensurate with a classification of 'OFFICIAL' under the Government Security Classifications Policy. No personal data is captured, processed or stored.