Cabinet Office

Assurance and Accreditation Approach for: Civil Service Pensions Service (CSPS)

Introduction

The Commercial Information Assurance (IA) team within the Cabinet Office (CO) provides IA support and expert advice to cross department/public sector projects and procurements where the CO acts as the Framework Authority, contracting or co-ordinating Authority. We ensure appropriate security requirements are identified and appropriate controls are included in the contract, implemented and managed throughout the contract term.

The CSPS is replacing the current administrator (MyCSP). The procurement exercise began in 2022 and Capita was selected as the new provider in November 2023 with services due to commence in December 2025. Transition activity has been underway since December 2023.

Security of the CSPS data has been considered at all stages of the procurement process and is seen as a crucial element of both the transition work and the future business as usual operational service. The IA Team within the CO will continue to provide independent assurance for the programme team, Scheme Manager and on behalf of our participating employers.

For the CSPS, the Commercial IA team has been supplemented by an external Information Risk and Cyber Security Specialist Consultancy Service as well as Security Architects from within the CO. The team is led by Anna Brostromer, Head of Commercial Information Assurance. This paper outlines the approach the team is taking to ensure the CSPS is implemented securely in accordance with the contractual security requirements. We are aware that as Joint Data Controllers, participating employers want reassurance that data security is at the top of our agenda, and that the risk profile is being monitored throughout the life of contract.

CSPS Security Assurance Approach

Requirements Capture

Before the procurement had started, the IA team already had a thorough understanding of the sensitivity of the pensions data as they'd undertaken the security assurance for the current pensions service with MyCSP.

Due to technology changes and the greater use of cloud-based services and hosting, we approached the more sensitive HMG departments to understand their specific security requirements and potential red lines, particularly with regard to locations for data hosting, the use of cloud services, remote working, and clearances for staff with access to the data. We also asked for any specific security requirements departments may have in relation to their staff's data records.

Drafting Procurement Documentation

Based on the discussions with departments we agreed a risk appetite for the new service provision and started work on drafting the security elements of the procurement documentation to ensure these requirements were reflected at all stages of the process. This included input to the Selection Questionnaire, the Evaluation questions and the Security Schedule to be included in the contract. An external legal firm with expertise in public sector procurements assisted with this drafting.

All elements of the new service are to be hosted within the UK, with no off-shoring of support or other administration services. UK-based cloud platforms were considered to be an acceptable option with strict security controls, including a separate environment, also known as a "tenancy" for the CSPS.

Limited remote working (working from a location other than the office) was also allowed for administration staff who do not have access to the bulk data set – that is, they cannot access more than five member records at a time. This remote working acceptance to align with current working practices.

Bid Evaluation and Negotiation

We held several negotiation sessions with bidders so that they understood our risk appetite, the complexities of the stakeholders who participate in the scheme and the risks of penetrating our data set. The Commercial IA team was involved at all stages of the procurement process.

Transition and Implementation Activities

The IA Team set up a Security Working Group (SWG) with Capita to agree on all the security deliverables involved in securing data during the transition period. This has to date included:

- agreeing the security protocols for an initial transfer of data for testing from the incumbent supplier;
- the anonymisation protocols to allow the data to be used for testing – we want to minimise the use of Personal Identifying Information (PII) as much as possible. To this end, we have asked for migrated data cuts to be anonymised during the testing phase;
- agreeing the design and testing requirements for the initial data storage environment;
- reviewing the high-level design for the full production solution.

The IA Team are also involved in ongoing activities including agreeing the Risk Assessment and Security Management Plan (SMP) for the final implementation. We have had detailed discussions on the specific controls around remote working and which supplier functions should be allowed to work remotely. The approach to security testing and remediation has been agreed. The final version of the SMP will require agreement from the Authority (CO) on the adequacy of the controls to reduce the risks to an acceptable level to meet the risk appetite of **Cautious -** https://assets.publishing.service.gov.uk/media/61239758e90e0705481fc085/20210805_-_Risk_Appetite_Guidance_Note_v2.0.pdf.

Business as Usual

Once the CSPS is fully transitioned to the Capita solution, the security and information assurance aspects will be managed through the SWG. Any change requests will also be managed via this group which will meet at least monthly.

The SWG will agree the requirements of an annual penetration test by a CHECK approved supplier with remediation of any vulnerabilities found closely monitored. The patching status of the solution will be monitored to ensure it meets the contractual requirements and any security incidents or breaches will be managed by this group.

The SWG will report to the Contract Management Group which is the escalation route for any issues that cannot be resolved.

Feedback

Employers can share this document with their Information Assurance, Security or Data Protection colleagues.

If you have any queries or would like more information, please contact us via the feedback link on the microsite