Government
People Group

Cabinet Office

Future Pensions - CSPS

Security Presentation

August 2025

Introduction

- CO are doing the Information Assurance work for the Future Civil Service Pensions Scheme that will be a managed service provision from Capita. This is the same approach used for the existing pensions service from MyCSP/Equiniti.
- This presentation will set out:
  - our approach to security assurance for the new scheme and
  - provide an overview of the work we are currently doing.
- And is solely about the CSPS service and not about the Remedy solution which is being implemented separately to resolve the McCloud judgment.

Government
People Group

Cabinet Office

Cabinet Office Information Assurance Team

- The IA Team is independent from the Authority and is part of the Commercial Team in the CO. This is important to enable us to provide independent advice and recommendations to the Authority on security risks and issues.
- The Team consists of:
  - Anna Brostromer (Head of Commercial IA, CO Commercial)
  - Sarah Barclay (Accreditor and CO Information Assurance Adviser)
  - Chris Botticelli (Security Architect, CO)
  - Paul Allen (Cyber Security Consultant, Actica)

We aim to cover:

- The procurement process from a security perspective
- Security Working Group (SWG)
- The contractual security requirements
- The Information Assurance evidence required from Capita before transition
- The current status of the assurance activities

Security Involvement in the Procurement of the New Scheme Administrator

- The IA team was involved from the outset of the programme.
- A robust security schedule was provided to all potential bidders to ensure they knew what security requirements needed to be met.
- A Risk Appetite Statement was provided to potential bidders. The risk appetite was set as Cautious and made it clear that all risks above Low would need to be mitigated.
- Security questions were included in the SQ process.
- Detailed security questions were included in both the ITT phases.
- The IA team was involved in the negotiation process with input from GCHQ on security matters.

Security Working Group (SWG)

- The joint Capita/Cabinet Office SWG was set up on contract signature to manage all aspects of the security assurance throughout the transition and implementation phases.
- The SWG is responsible for ensuring:
  - A full information risk assessment is done
  - A secure architecture is being implemented
  - All activities as part of the transition and implementation are assessed from a security perspective and the risks are well understood by the Authority.
  - The security controls are suitable to reduce the risks from the risk assessment
  - The delivery of all agreed security documentation.
  - The transfer of various tranches of data sets from old and new supplier are securely managed.

Contractual Security Requirements

- The Commercial IA Team worked together with external legal counsel to produce a robust security schedule.
- This was an adaptation of the Model Services Contract - Accreditation Schedule, to meet the specific requirements for the CSPS and included clauses to ensure that any red lines provided by our more sensitive departments were met.
- These additions included very specific limitations to homeworking and offshoring.
- All aspects of CSPS service are hosted, processed and managed within the UK.
- Homeworking had to be allowed due to TUPE issues, as staff transferring from MyCSP have been since COVID. However, access to bulk data sets is not allowed from home workers or system administrators apart from in very specific circumstances and the security controls around these exceptions must be agreed by the SWG.
- The CSPS is considered to be an OFFICIAL Sensitive solution. However the CO IA Team were well aware of the issues around aggregated bulk data from particular employers.

Documented activities required by the security schedule

- Risk Appetite Statement - produced by the Authority
- Assurance Plan
- High Level Design architecture
- Security Management Plan
- ITHC Scope
- ITHC Report and Remediation Plan
- Residual risk statement - produced by the Authority

Government People Group

A Security Management Plan which includes:

Cabinet Office

- An agreed diagram of the scope of the Supplier Information Management System
- A formal Information Risk assessment and Risk Treatment Plan
- An ISO 27001:2022 Statement of Applicability
- Risk register
- Security controls
- Third party suppliers list and the process for managing those third parties.
- Assessment against Secure by Design principles if required
- Support register of hardware and software
- Module register of third party software

- Module register of third party software
- Change register - to be populated later
- An assessment of the SIMS against the security requirements in the schedule
- Register of site and support location
- Backup and recovery plan
- Incident reporting process
- Agreed remote working policy
- Agreed Protective monitoring process
- Retention periods for audit records and event logs
- ToRs for the Security Working Group (SWG)
- Evidence of Information Assurance certifications

Current Assurance Activities - Status

- High-level Design agreed
- Draft Security Management Plan (SMP) agreed - to be updated.
- Information Risk Assessment completed and Risk Register being updated as identified risks are reduced.
- Initial ITHC completed with remediation work underway. A second test will be done as more functionality is rolled out.
- Transfer mechanisms for the data agreed and assured SFTP and Databox
- Homeworking arrangements agreed (5 records).
- SOC/SIEM alerting and reporting still under discussion.
- Final testing with anonymised data to test calculations under approval process.
- Physical site security arrangements reviewed and approved.
- Printing facility visited and approved.
- Security clearances underway.

Government
People Group

Cabinet Office

Questions?

Anna.brostromer@cabinetoffice.gov.uk