Question	Answer
How confident are the team that Capita will be ready for the transition from a security perspective?	From a security perspective, we are confident that the team will be prepared for the transition. The testing undertaken so far gives us a strong level of assurance. However, there are some areas that require further attention to ensure full readiness. Overall, we believe that the security measures associated with the Capita solution will be an improvement over the current arrangements.
A slide stated that an "Information Risk Assessment" has been completed, Did the "Information Risk Assessment" explicitly cover personal data, including mandatory DPIAs and Data Processing Agreements under UK GDPR? If not, when and by whom will this governance be addressed? Has a DPIA been completed, what risks were identified, and how have they been mitigated? Which DPO approved the DPIA?	The DPIA is almost complete and in final stages of review. We're hopeful this will be able to be shared by the end of September.
Please could you advise when we may have sight of any security risk assessments? We'll need to run these past our internal cyber security folk. The draft SMP would also be super helpful	We are unable to share the full Security Risk Assessment with all employers due to security sensitivities, particularly relating to additional requirements from more sensitive departments and organisations. However, we are happy to arrange a call to discuss the residual risk statement, outline the findings from the penetration tests, and explain how these risks have been mitigated or remediated.
Can you please confirm that Capita will have the ability to receive and process password protected pension files?	We will confirm officially, but the solution being implemented by Capita is delivered via a secure portal protected by password and MFA. As such, password protection of files may not be necessary, since files will be securely transferred through this portal. We will clarify whether password protection can still be applied and provide a definitive response.
Does your work also cover the 'non-production' system as well?	Yes, it does. It's all in the same tenancy.

Following go-live, will CAPITA disclaim responsibility for any queries concerning COMPENDIA data? If so, what security considerations must be addressed when extracting existing data from MyCSP, and is it necessary for employers to obtain and maintain their own copy of this data?	Following go-live, Capita will assume responsibility for ongoing queries related to data corrections and other issues. Any ongoing work or outstanding data queries currently handled by MyCSP are expected to be transferred as part of the cutover exercise. There may be a short period (approximately one to two days) when no data is exchanged with MyCSP to ensure a smooth transition over the weekend. After this period, cases will be loaded into Capita's Work Management System and, due to TUPE arrangements, are likely to be managed by the same staff. Additionally, all phone call recordings and imagery data will be transferred accordingly.
When will we have more information on the system/portal that will be used for monthly file transfer i.e., system replacing Connect as we will need to do a SIA internally and this can often take some time?	There is already a lot of information available on the transitional microsite. Please see link here. There are training sessions which are open to be booked, in addition to the documents/guides/process maps which are there to help people with that expect.

Will GPG manage the security of the contract with capita and how will ongoing assurance be provided to depts going forward?	The contract includes clear requirements for a security working group, outlining how the authority and Capita will collaborate on security matters. The GPG security team will be involved in ongoing assurance activities throughout the contract, with monthly meetings to discuss security change requests, testing, and other relevant issues. The pensions team in GPG will serve as contract managers, while the security team will act as independent verifiers within the Security Working Group. Capita will be expected to provide annual assurance and accreditation. Additionally, a residual risk statement will be maintained and regularly updated. During each Security Working Group, we will review the current risk landscape, oversee incident management, and ensure continuous oversight of system and service security throughout the contract duration.
My question is we already have extensive security schedule as part of government, so how does this security schedule differ from what we currently have and specifically done for this?	We were unable to utilise the modular security schedules initially, as they were not fully developed for the new pensions contract. However, we have retrospectively incorporated similar clauses into the contract during its drafting. Additionally, we have made some minor adaptations to address all home working arrangements and include remediation clauses, such as provisions for withholding charges, edge clauses, and the involvement of an independent cybersecurity consultant, to ensure comprehensive security management specific to this contract.
Will we be able to see the security schedule and only the security schedule part of it so that it gives us an idea what the point is that we have thought through so that we could try and incorporate in any of our own areas?	The Security Schedule is viewed on Contracts Finder.

The artefacts you've described in the security management plan, are they available?	The security management plan can be made available for viewing under controlled circumstances. However, due to its sensitive nature, it can only be shared with the more sensitive departments and not with all departments. It is a highly sensitive document and must be handled appropriately.
When sharing the risk assessment what do you consider the most sensitive orgs you will share this with, as all the data is sensitive personal information for every organisation, will you share a summary of the assessment to give assurance to all organisations? And the organisation is responsible under the DPA 2018 for ensuring the personal information is protected	The most sensitive departments, such as the MoD and FCDO, are considered high-priority regarding sensitive data; however, all data involved is classified as sensitive personal data. We will need to determine which information can be shared more broadly, especially considering potential national security concerns. Please note that, while all data is regarded as sensitive, we will share the residual risk statement to provide assurance on risk management. If you require further detail (within reason), there may be an opportunity to review the relevant documentation in the Cabinet Office, subject to appropriate access arrangements. This would allow you to understand the measures we have implemented.
Hopefully, we won't have another Covid in the near future but have you considered any contingencies (e.g. ramp up of remote working) in case of a future pandemic?	In light of TUPE considerations, homeworking has been facilitated, and most of Capita's staff are already working remotely. However, certain restrictions are in place. For example, technical limitations currently allow only five records to be accessed at a time, meaning some roles, such as database administrators, may need to perform certain duties onsite. In the event of another lockdown or similar scenario, we would enable employees to work from home, subject to these technical restrictions. Additionally, all personnel working on this contract are minimum SC cleared, and working without this clearance is not permitted.

Will any of the third party suppliers have access to the data?	Some third-party suppliers, for example Intellica, are involved in the transition phase, providing data transformation services. All such suppliers are SC cleared. Additionally, Azure is a third-party provider, as this is a cloud-based solution hosted within its own tenancy; however, they will not have access to any of the data. The print supplier is part of Capita and will have extremely limited access, as the printing process is fully automated with minimal opportunity for data access.
You have not mentioned off shoring data and how these aspects are being considered from a security point of view?	There's no offshoring within CSPS contract, everything is UK based.
Will Capita home workers using managed devices & VPN?	Yes, Capita home workers will use managed devices and VPN connections. The VPN to be utilised is scheduled for a second IT health check in September. Additionally, all devices are managed and have been included in penetration testing to ensure security.
I am not sure if this was mentioned and I missed it, when it comes to assurance - will you take a continuous assurance approach (through SWG or other forums/means) or will there be a "regular/annual" kind of assurance process? Also, how about auditing requirements? does anyone still do "in person" auditing/ or using 3rd parties to conduct them?	Absolutely. This is a priority for us. We will not rely solely on annual assurance meetings. Instead, we will hold monthly Security Working Group meetings throughout the entire contract duration to review security posture, discuss change requests with security implications, and track remediation efforts. Capita is responsible for third-party assurance activities and will provide evidence of these assurance processes, including details of the third parties involved. Additionally, we will conduct ongoing audits where necessary, including physical security inspections at locations, review of security policies, and assessments of how security controls are being implemented. This

	continuous approach ensures rigorous and proactive security assurance rather than a solely periodic process.
How will breach management be implemented, I assume that Capita will inform your team immediately of a breach, will you then communicate a limited alert to all the organisations. By limited I mean just that there has been a breach, but not the details until we may need to know?	This process is still being signed off. Without going into the detail until the process has been signed off, but typically that is how it would work
What is the duration of the contract with Capita?	7 + 3
You said the duration of the contract is 7 + 3. Does that mean 7 years with an option to extend for a further 3 years?	Yes
Will the employer and employee telephone helplines also be managed by some Capita staff in India or is this still in Liverpool? I think I may have missed this one, apologies	The contact centre will remain in the UK. All work on the CSPS contract will remain in the UK.
What data sharing governance is being put in place?	The Cabinet Office as the Scheme Manager is the primary data controller, while each employer is a joint data controller responsible for collecting and keeping their employees' pension data accurate and securely transferring it to the Scheme Administrator (Capita) in accordance with agreed timescales and GDPR. Current details of responsibilities can be found in Stakeholder charter which is in the process of being updated.

That was a very good presentation. It's not particularly about the current security working group, which seems to have everything all in hand and it's really about the changes. So employers on and infrastructure. What kind of notification change management for any of the developments for automation and digital tools that Capita are due to introduce will organisations get so that they've got time to test plan?	There is already a lot of information available on the transitional microsite. Please see link here. There is training sessions booked as well are open to be booked on as well to help people with that aspect.