OFFICIAL SENSITIVE

UCPB180517 – BTL05

To: UC Programme Board Members

From: **Anthony Brigginshaw**
Sponsor: **Ian Wright**
Author: **Rob Thompson**
Date: **9th May 2017**

Copy: **Claudia Natanson**

Update on Security Risk Register for UC Full Service

- **To update Programme Board on the latest position regarding the UC FS security risk register as of 12th April 2017.**
- **To note the acceptance, by Programme Delivery Executive (PDE), of the five UC FS red risks and their associated mitigation plans.**
- **To note the exposure of the Programme to three DWP Enterprise level red risks which need to be mitigated outside of the programme before scaling in October 2017.**

Introduction

1. The purpose of this paper is to outline the latest security risk position for UC Full Service based upon a risk register agreed by the programme and Chief Security Officer (CSO) from 12th April 2017.

2. The scope of the work was to validate critical risks and to identify & specify risk treatment plans to mitigate these risks. The brief was to ensure no critical residual risks remained for scaling in October 2017.

3. The work was led by the CSO risk analyst team who are now embedded into the UC Full Service multi-disciplinary team, providing security risk expertise to the programme and independent oversight of risks and associated mitigations to the CSO.

4. The work was performed using the Department's Enterprise Security Risk Management process and protocols, the standard used by the CSO organisation for all departmental security risks. It is noted that this mode of operation will be used in future to identify security risks and endorse risk treatment plans, continuing independent scrutiny of risks and mitigations outside of the programme's core functions.

Current position

5. The work identified 1 current risk with a planned mitigation and 4 future risks which will be designed out of the system through the migration to Amazon Web Services (AWS) cloud hosting. These 5 risks and mitigations are all owned within the programme.

6. Status updates, progress reporting and validation of mitigations are now under the scrutiny of the department's ESRM process as well as being tracked within the programme for these 5 risks.

7. The work also identified 3 additional current risks owned outside of the programme by Digital group which could significantly impact the programme if not mitigated.

8. It will be necessary for the programme to work with Digital to ensure that these dependent risks are sufficiently mitigated to ensure a safe and secure approach to scaling post October 2017.

9. The Programme Delivery Executive accepted the current status of the red risks and associated mitigation plans and requested that regular updates on the position of these risks are made visible leading up to October 2017. They also remarked that the current risk profile and progress on mitigation plans is to be as expected for a programme of this size and scale at the current time, and that this did not prompt anxiety about scaling in October.

Summary

10. This paper has been brought to this meeting to make visible:

- The latest position on critical risks for UC FS
- The acceptance of the current risk position for these risks at Programme Delivery Executive
- Transparency of programme exposure to Enterprise level security risks that require mitigation outside of the programme itself.

Decision / Recommendation

- For information only.

Timing

As a below-the-line paper for the Programme Board meeting on 18th May 2017.

Annex 1 – List of risks and mitigations

Risk ID	Risk Description	Residual Rating	Mitigation/Controls Planned
UCDS-159	There is a risk that servers, security appliances and EUD builds are out of date on the development network and could contain vulnerabilities allowing an external threat actor to steal sensitive technical information or utilise access as a stepping stone to the production environment where claimant details are stored.	20 (Red) (5 Impact) (4 Likelihood)	a. Remediation of ITHC finding is ongoing as of 7th April 2017. b. Change control process documented on Confluence to ensure that every configuration change is raised on JIRA and received the right approval. Firewall changes are reviewed by the Release Management Team and approved by Senior Managers. c. SSOC Protective Monitoring Solution implemented as MVP – w/c 13/03 March 2017. It is expected that once controls have been implemented, this risk will be reduced as follows: Impact = VERY HIGH (5) Likelihood = LOW (2) Final Risk = HIGH (10)

Risk ID	Risk Description	Residual Rating	Mitigation/Controls Planned
UCDS-084-2	There is a risk of data loss through the transmission of data over unencrypted links between AWS availability zones.	20 (Red) (5 Impact) (4 Likelihood)	Prior to deployment on 27th May 2017, the expected AWS model will have TLS encryption between micro services and because of this between availability zones. This will be tested by independent CHECK approved Pen Testers starting 18th April, 2017. This will reduce the risk of data being intercepted by AWS Privileged User as the data will be encrypted. Given the Threat Actor in this case is an AWS Privileged User, it is felt that the Likelihood should be Low (2).

Risk ID	Risk Description	Residual Rating	Mitigation/Controls Planned
UCDS-084-3	There is a risk that an AWS privileged user could access physical devices to harvest claimant sensitive data, NINO, Bank Acct etc.	20 (Red) (5 Impact) (4 Likelihood)	a. Work to encrypt UCFS data using AWS Cloud Hardware Security Modules (HSM) is on-going as of 7th April 2017. Date for completion is 31st October 2017. Tony Gaunt is responsible for the delivery of this activity. AWS staff do not have access to manage encryption keys within the Cloud HSM service. This reduces the risk of an AWS Privileged User decrypting UCFS data. b. AWS Key Management Service (KMS) will be used to encrypt all data at rest (DAR). Whilst the KMS service does encrypt data, encryption keys are managed by AWS staff. The residual risk for this control is therefore that an AWS Privileged User who has access to encryption keys could use it on UCFS data. Given the Threat Actor in this case is an AWS Privileged User who has access to the physical device, it is felt that the Likelihood should be Low (2).

Risk ID	Risk Description	Residual Rating	Mitigation/Controls Planned
UCDS-086	There is a risk that claimant information could be disclosed through the inappropriate configuration or patching of the DWP controlled elements of the UCFS infrastructure within AWS.	20 (Red) (5 Impact) (4 Likelihood)	a. Currently outstanding Infrastructure vulnerabilities are expected to be completed prior to go live (27th May 2017), and a further ITHC will be conducted from 18th April 2017 to validate that these have been fully remediated. b. Current outstanding Application vulnerabilities have been pushed forward for prioritisation. c. Going forward, on going independent testing of service will be carried out annually as a minimum, with a stretched target for 1/4ly tests. Internal testing will also be carried out to ensure that vulnerabilities are caught during the development processes. IT Strategy required, this is on the To-do list but not yet planned at the time of reviewing the risk with the responsible delivery manager (Tony Gaunt) on 7th April 2017. The above controls will reduce the risk of vulnerabilities being present. It is expected that once controls have been implemented, this risk will be reduced as follows: Impact = VERY HIGH (5) Likelihood = LOW (2) Final Risk = HIGH (10)

Risk ID	Risk Description	Residual Rating	Mitigation/Controls Planned
UCDS-166-2	There is a risk that unless technical vulnerabilities are remediated prior to migration (to AWS) a third party, Internet based attacker, will exploit one or more vulnerabilities within the UCFS environment to gain access to UCFS Claimant Data or impact services.	20 (Red) (5 Impact) (4 Likelihood)	a. Vulnerability expected to be resolved as part of ongoing work. High findings in the Dec 2016 ITHC, are expected to be resolved prior to migration (to AWS) in May 2017. Tony Gaunt is the technical lead responsible for the delivery of this activity by 31st May 2017. It is expected that once the identified vulnerabilities have been fixed, this risk will be reduced as follows: Impact = VERY HIGH (5) Likelihood = VERY LOW (1) Final Risk = MEDIUM (5)

Risk ID	Risk Description	Residual Rating	Mitigation/Controls Planned
UCDS-093	There is a risk that the misuse of web-based COTS (commercial off the shelf) products such as Google forms, online surveys or tools used to collaborate such as Trello or Slack could result in personal data being leaked either via cross scripting attacks or by cross site forgery requests.	16 (Red) (4 Impact) (4 Likelihood)	• This risk is being managed at enterprise level by D-SRAF. "Digital Hubs Use of Personal/Non-Standard Devices and Applications" D-SRAF actions 5.4.17/15, 5.4.17/16 and 5.4.17/17 refer: a. Meeting arranged to scope out controls testing around non-standard devices and applications. b. Review the scope of the risk assessment which currently focuses on 330 staff with open devices and 164 with personal devices in digital hub locations. c. For use of personal/non-standard devices and applications. An exception to the Acceptable Use Policy has been submitted for Slack. Investigate CRC tracing where Slack is being used and the options available to detect unapproved devices being connected to the network. (Risk Action Owner – **Redacted**)

Risk ID	Risk Description	Residual Rating	Mitigation/Controls Planned
UCDS-136	There is a risk that a persons NINO is divulged within Central Payment System produced 3rd party reports and payment files (remittance advice) and could be used by an threat actor to pose as the person to gain access to many DWP and other Government Departments services.	20 (Red) (4 Impact) (5 Likelihood)	a. For client payments the NINO has already been removed from Automatic payment system, manual systems still show NINO. b. For payments to Landlords – it was suggested that removal of the NINO is automatic payments was on the backlog but this is not the case. c. For payments to other 3rd parties the problem still exists. With the controls in place the Likelihood is reduced to High (4); however this is very much an issue for CPS and not UC FS. Agreed during the Risk Analysis workshop on 3rd April, 2017 that all the mitigation controls to be implemented still need to complete to reduce the Likelihood. However, email dated 3rd April 2017 from **Redacted** (CPS) stated that this is not solely a CPS risk and should be a DWP business-wide issue. (Risk Action Owner - **Redacted**)

Risk ID	Risk Description	Residual Rating	Mitigation/Controls Planned
UCDS-193	There is a risk that Protective Monitoring controls will be ineffective during UC FS Scaling and alerting of unusual events will go unactioned.	16 (Red) (4 Impact) (4 Likelihood)	Ad Hoc D-SRAF meeting is scheduled for the 20 April 17 to review Protective Monitoring. D-SRAF Action 1/3/17/15 refers. a) Recruitment of PM specialists are being progressed. b) Support and Maintain will be progressed by IOS, this will be monitored via the D-SRAF. c) Priority of PM will be determined shortly, top 5 services will be monitored. (Risk Action Owner - **Redacted**