FUJ00211295

From: "Matthew.Lenton GRO

Sent: Thur 20/06/2019 9:02:49 AM (UTC)

To: "ParkerSP GRO , "pete.newsome GRO GRO , "Mark.Wright GRO "John.Simpkins GRO GRO

Cc: "Dave.Ibbett GRO

Subject: RE: Queries arising out of Dr Worden's evidence - URGENT [WBDUK-AC.FID123944863]

Steve,

Sorry, I failed to spot to that you had failed to answer the exam question…

Q: Privileged User Access logs - Is there anything worth looking at or referring to in the PUA logs **from 2015 to present**?

A: We don't believe that the logs help here because up to July 2015 we only logged obtaining and relinquishing privilege.

Matthew Lenton
Post Office Account Document Manager
Business & Application Services

Fujitsu
Lovelace Road, Bracknell, Berkshire, RG12 8SN
Phone:
Email: GRO
Web: https://www.fujitsu.com/global/

From: Jonathan Gribben GRO
Sent: Thursday, June 20, 2019 8:11 AM
To: Lenton, Matthew GRO
Cc: Lucy Bremner GRO ; Katie Simmonds GRO ; Michael Wharton GRO ; Parker, Steve GRO ; Newsome, Pete GRO ; Ibbett, Dave GRO
Subject: RE: Queries arising out of Dr Worden's evidence - URGENT [WBDUK-AC.FID123944863]

Matthew,

Thank you for the responses, which we are discussing with Counsel.

One immediate follow up point – the question about privileged user logs is whether there is anything useful in the logs from 2015 to the present day. Your response relates to the pre-2015 logs. Please would you let me know if there is anything worth looking at or referring to in the 2015 to present day logs.

Kind regards

Jonny

Jonathan Gribben
Managing Associate
Womble Bond Dickinson (UK) LLP

d: GRO

FUJ00211295

m: GRO
t:
e:

Manage your e-alert preferences

WOMBLE BOND DICKINSON

womblebonddickinson.com

From: Matthew.Lenton[GRO]>
Sent: 19 June 2019 11:56
To: Jonathan Gribben[GRO]
Cc: Lucy Bremner[GRO]; Katie Simmonds[GRO]; Michael Wharton[GRO]; ParkerSP[GRO]; pete.newsome[GRO]; Dave.Ibbett[GRO]
Subject: RE: Queries arising out of Dr Worden's evidence - URGENT [WBDUK-AC.FID123887118]

Jonny,

Please see the responses added below, and the attachments to which they refer.

Matthew Lenton
Post Office Account Document Manager
Business & Application Services

Fujitsu
Lovelace Road, Bracknell, Berkshire, RG12 8SN
Phone:
Email: GRO
Web: https://www.fujitsu.com/global/

From: Jonathan Gribben [GRO]
Sent: Tuesday, June 18, 2019 12:15 PM
To: Newsome, Pete [GRO]; Lenton, Matthew [GRO]; Ibbett, Dave [GRO]
Cc: Lucy Bremner[GRO]; Katie Simmonds[GRO]; Michael Wharton[GRO]
Subject: RE: Queries arising out of Dr Worden's evidence - URGENT [WBDUK-AC.FID123887118]

Hi all,

One more request:-

- **Controls around remote access** – Green took Worden to some examples of the two pairs of eyes policy not being followed:-
    - OCP 21918 (raised by and monitored by Anne Chambers)
    - OCP 23896 (raised by and monitored by Anne Chambers)

FUJ00211295

- OCP 26361 (raised by and monitored by Vishnu Ramachandran)

Is there a reason why the policy was not followed in these examples?

[Lenton, Matthew] In his cross-examination PG has been incorrectly interpreting the information in the "Monitored by" section of OCPs. His interpretation is that this records the name of the person who witnessed the change in the context of the "four eyes" rule, when in fact, the "Monitored by" field was used to record the person or team that would monitor the effect of the OCP, in particular where the OCP would affect the live service. See CS/PRD/019 2.2.

The "four eyes" rule was (and is) only mandated for changes that impact the financial integrity of the system. The change vehicle for these was (in the vast majority of cases) an OCR which will record the name of the person who witnessed the change in the context of the "four eyes" rule. Where an OCP was used, the name of the person who witnessed the change would be explicitly recorded in one of the updates since the OCP system did not have a specific field for this purpose.

See CS/PRD/019: Section 2.2: on the use of "Monitored by": *"Complete the "Responsibility for Monitoring" box. This should specify the name of the person(s) or team(s) who have the responsibility for monitoring the effect of the OCP once implemented. In particular the monitoring should be checked that there is NO detrimental effect on the "Live Service". If necessary the details of the monitoring to be undertaken can be specified in the "Details & Purpose of Change" section."*

CS/PRD/019: Section 6.0:

On the differences between the OCP and OCR processes and how they are used:

"The OCR process involves the correction of customer data on the live system, and because user data is involved, requires different approvals and auditing

Only the SSC has the authority to make changes to the data on the system, and therefore only SSC staff can action an OCR .

In most cases, an OCR does not involve the financial integrity of the system. Under these circumstances one of the SSC Manager, the Support Services Manager or the Customer Service Duty Manager can approve an OCR. If the data to be changed has a financial impact on Post Office, then approval must also be given by a senior Post Office Manager.

When an OCR has been approved, and has been actioned, it is necessary for two users of the OCP system to confirm that the work has been done – an actionee and a witness. The actionee will always be an SSC staff member, the witness can either be an SSC staff member or a development staff member."

On the specific OCPs above:

a) OCP 21918 (raised by and monitored by Anne Chambers)

Actioned by Anne on 03/03/2009 09:32.

As explained above, this would be a manual process as the OCP does not have a witness field (the OCRs do).

Looking at the OCR relating to the same Peak (PC0175821) you can see the Witness field used:

Approval

Approved by Mik Peach (19/02/2009 12:29) for POA SSC Support

Action

Actioned by Catherine Obeng (02/03/2009 17:16) for POA SSC Support

Witness

Witnessed by Anne Chambers

The evidence is still attached to the Peak and we can see that the inserted messages are recorded there (before insertion and the resultant messages afterwards).

FUJ00211295

These messages have the identifier tag (<Comment:PC0175821>) attached to demonstrate where that have been created.

There is also an email chain which shows that Anne will contact the SPM before and after the correction, which is scheduled to be done at the quietest time of day.

Overall we believe that such a substantial change would have been witnessed but there is no proof on the OCP that it was, however the SPM was kept in contact while the change was made and all changes have been recorded on the Peak to allow them to be reviewed.

b) OCP 23896 (raised by and monitored by Anne Chambers)

Raised by Anne on 16/10/2009, actioned by Anne on 28/10/2009

This change is for a migration object and is not financially affecting so does not need to be witnessed.

c) OCP 26361 (raised by and monitored by Vishnu Ramachandran)

Vishnu raised the OCP on 14/04/2010

Ed Ashford actioned the OCP on the same day.

His output is shown in the OCP:

Ed Ashford (Core Services Unix Support) wrote at 14/04/2010 18:32: Change committed after confirming output with development.

Kind regards

Jonny

Jonathan Gribben
Managing Associate
Womble Bond Dickinson (UK) LLP

d:
m:
t:
e: GRO

Manage your e-alert preferences

WOMBLE BOND DICKINSON

womblebonddickinson.com

From: Jonathan Gribben
Sent: 18 June 2019 12:07
To: pete.newsome GRO 'Matthew.Lenton GRO
Dave.Ibbett GRO
Cc: Lucy Bremner GRO Katie Simmonds GRO

FUJ00211295

GRO Michael Wharton GRO GRO
GRO
Subject: Queries arising out of Dr Worden's evidence - URGENT [WBDUK-AC.FID123887118]

Hi all

There are some points arising out of Robert's evidence last week that we'd like some further information on please:

- **Service audits eg F/1041 attached**:
    - [1] Is there a document setting out how the control objectives are decided/defined. It was put to Worden that Fujitsu define the control objectives. It would be helpful to know to what extent, if at all, this is true and if so, what process was undertaken to select these control objectives.

[Lenton, Matthew] Yes, that is correct, as stated in the letter from Ernst & Young contained in the report says: *"Fujitsu is also responsible for providing the services covered by the Description, specifying the control objectives, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the Assertion and designing, implementing and documenting controls to achieve the related control objectives stated in the Description."* ***It goes on to state*** *"A reasonable assurance engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the control objectives stated therein and the suitability of the criteria specified by the service organisation and described in the Assertion."* ***So E&Y check and confirm that the definition of the control objectives is suitable.***
The objectives setting was however done in discussion with and by agreement with Post Office: the attached document "2011-10 SAS70 Audit presentaion BM.pptx" is an early presentation (we believe it to be an internal presentation to the then Fujitsu Account leadership, but it shows the process) putting the case for providing a SAS70/ISAE3402 report, and which shows that the controls would be based on those that other standards-based audits had reported on previously; a more fully worked out update was presented to POL on the attached "2012-09 POA EY ISAE3402 Update for PO Ltd".

    - [2] Which provisions of the service audits are relevant to remote access (privileged users, SSC inserting transactions etc.). It was put to Worden that the service audits do not cover issues that are relevant to remote access. Any control objectives that do address aspects relevant to remote access would be useful.

[Lenton, Matthew] In the report that you attached, Control Objectives 10, 11, 13 are relevant.

- **Privileged User Access logs -** Is there anything worth looking at or referring to in the PUA logs from 2015 to present? Is there a way of demonstrating that privileged users have not edited or deleted transaction data or added transaction data.

[Lenton, Matthew] We don't believe that the logs help here because up to July 2015 we only logged obtaining and relinquishing privilege.

- **APPSUP -** which table(s) could it write to?

[Lenton, Matthew] The short answer is that the APPSUP role can do anything to any schema in the branch database. A detailed list is in the attachment "APPSUP_role.txt".

- **The Transaction Correction Tool -** please review the questions and answers set out on Day 20, pages 159 to 160. Is what Worden says here true? If not, why not?

[Lenton, Matthew] Please see comments appended to the attached version of the transcript.

As the deadline for closing submissions is fast approaching, please would you get back to me by midday tomorrow. If you think that is going to be an issue, please let me know ASAP.

Kind regards

Jonny

FUJ00211295

Please consider the environment! Do you need to print this email?