WBON0001487

From: Johann Appel <GRO>
To: Angela Van-Den-Bogerd GRO, Ben Cooke GRO
Cc: Catherine Hamilton GRO, Lucy Bremner GRO
Subject: RE: URGENT PLEASE- Information needed for GLO Horizon issues Trial
Date: Tue, 6 Nov 2018 10:35:56 +0000
Importance: Normal
Inline-Images: image010.png; image011.jpg; image012.png; image013.png; image014.png; image015.png; image016.png; image001.jpg

---

Hi Angela,

Lucy has informed me that Thursday 8 November is the absolute deadline for this information. We are still waiting on RMG to search for their archives for documents related to the FY2010 ARC and EY report.

It is important to note that the 2011 EY report in question refers to the Credence issue only as part of an update of the 2010 audit findings. This means the audit finding was identified during the audit of the FY2010 accounts. In their 2011 report, EY actually state that the Credence application was out of scope for the FY2011 audit and they do not conclude whether the control issues identified in 2010 were remediated.

The approach I followed was to scrutinize subsequent audit reports, board minutes and audit committee minutes to identify if this control issue was re-reported. We reviewed the following documents:

- POL ARC 23 May 2012 – First official meeting of the new Board Audit committee following separation from RMG. EY audit results report presented at this meeting.
- POL ARC 13 November 2012
- POL Board Meeting 27 May 2011
- POL Board Meeting 4 July 2011
- POL Board Meeting 22 September 2011, also the POL IT Audit Update (SAS70) paper.
- POL Board Meeting 10 November 2011
- POL Board Meeting 12 January 2012

We found no reference whatsoever to Credence or specifically to change controls over the Credence application. Given that auditors report by exception, I conclude that the Credence issue was resolved or if any issues continued to exist, this was not significant enough to be reported to and actioned by the ARC or the Board.

WBON0001487

I will continue to chase RMG to try and find the original 2010 EY report and hopefully a confirmation in the 2010 ARC minutes that the controls issues were remediated.

Hope this helps.

Best regards,

Johann

Johann Appel
Head of Internal Audit

Ground Floor

20 Finsbury Street
LONDON EC2Y 9AQ

GRO

From: Angela Van-Den-Bogerd
Sent: 30 October 2018 19:52
To: Johann Appel <GRO>; Ben Cooke GRO
Cc: Catherine Hamilton <GRO>
Subject: FW: URGENT PLEASE- Information needed for GLO Horizon issues Trial

Hi Ben

Thanks for the response. Johann is pulling together a response on the Credence point. **Johann** - for completeness would you please touch base with Ben on this to ensure we have everything covered.

Thanks,

Angela

Angela Van Den Bogerd

Business Improvement Director

WBON0001487

1st Floor,Ty Brwydran,

Atlantic Close,Llansamlet
Swansea SA7 9FJ

GRO

Confidential Information:
This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorised review, use, disclosure or distribution is prohibited. If you are not the intended recipient please contact me by reply email and destroy all copies of the original message.

From: Ben Cooke
Sent: 30 October 2018 14:59
To: Catherine Hamilton <GRO>; Angela Van-Den-Bogerd <GRO>
Cc: Peter Stanley <GRO>; Michael Austin <GRO>
Subject: RE: URGENT PLEASE- Information needed for GLO Horizon issues Trial

Catherine, Angela

Apologies for the time taken to respond – it's taken me a while to have the time to get my head around the ask. I have some views on the below (which I've given) and I'm not entirely clear what argument the opposition are trying to make – which makes it hard to respond correctly, I'm happy to re-respond if more info can be provided. Unfortunately I'm almost stuck without Post Office's audit response doc.

What more can I do?

I've called a contact at CGI who was involved at that time. Once he gets back to me I will respond again.

Questions

Have we asked EY? For the audit response documents? Could we? If the data team or I could see it, then we could better respond on top.

Do finance store the audit response docs? They usually facilitated the IT audit points…

WBON0001487

What I've been working to is the section from Lucy as noted, "Jason Coyne, the Claimants' IT expert, refers to an audit document produced by E&Y in 2011 (see attached) which identified issues with the credence application, namely weak change controls within the back end of the systems allowing Logica developers (the third-party provider) to move their own uncontrolled changes into the production environment. He goes on to say that "further documentation to approve fixes and patches applied to Credence outside of the release process were lacking, therefore linking changes to issue tickets to record the original request for the bug fix was not possible".

We need to understand whether these comments are correct and whether anything changed in light of the report."

It's hard to comment accurately on times before I arrived in the organization but I know the CGI team who managed this service – and am reaching out to see if they have some info. I understand that Mark Hotson and co only arrived in Mar/Apr 2012 and hence also don't have anything from the time the audit was completed.

Things I can say:

General Comment

Credence is a data warehouse that takes information from Horizon and 3rd party sources and reports on it. I don't believe information is fed from Credence back into Horizon at any point – hence it would not have impacted Post Master financials. Here I'm not clear the point that the Expert Witness is driving at.

Credence did/does report on Horizon data – but Agents are also able to see this data through Horizon.

Credence back end change process

The auditors point out:

1. Access rights to the production environment and the database that *would* permit developers to move their own changes
    - Whilst access rights *allowed* this, it does not mean that it happened, or that there is actually a lack of control. Only that uncontrolled change *could* exist. There can be perfectly legitimate resources for these types of access to exist, and reactive/monitoring controls to ensure that they are not exploited.
    - I can state for certain that by 2016 CGI had change control and release processes as one would expect under ITIL with changes going through an approval process prior to being released into the live environment.
    - I will see whether I can get support from CGI to respond to this comment
2. Documentation to approve fixes and patches that are applied to Credence outside of the release process does not always exist
    - From the sample selected documentation was provided for some changes and not others. Without re-reviewing the selected changes it's hard to say the magnitude of this audit finding. It may be that certain basic settings did not require documentation. We would need to see the Post Office response to the audit.

Credence Front End change & configuration

These points relate to people creating/changing business objects reports which sit on top of the core data sources. It is not uncommon for super users within organizations to be able to create or amend reports and

WBON0001487

this is used by analysts to create new reporting.

As the report points out there should have been better controls around reports used for reconciliations (as opposed to business analysis – which is where the majority of new reports tend to be created). However it should be noted that whilst people technically could have modified tested reconciliation reports, there is no evidence that they did.

	Issue	Location	Background	Recommendation	Management Comment	Current Year Update
12	**Credence (back end) change process**	IT	During our walkthrough and testing of the change control procedures for the Credence application we became aware of the following issues: 1. Developers at Logica, the third party provider of application development and support for Credence, had access rights to the production environment and the database that would permit developers to move their own changes into the production environment. 2. Documentation to approve fixes and patches that are applied to Credence outside of the release process does not always exist. We were advised by Logica personnel that for a sample of four changes selected evidence of approval to move into production did not exist and that it would not be possible to link the changes to problem tickets to record the original request for the fix / patch.	Management should require that their third party service provider segregate the roles of developer and implementer. Management should also require that their third party service provider maintain complete and accurate records that support the requests for changes, testing of changes, approval to move into production and the separation of developer and implementer. Management should periodically audit the achievement of service level agreements.	This is clearly documented in OCP. There will be further work to look at requiring Logica to comply and ensure appropriate role separation. To be retested in 3 months.	Application not in audit scope for FY11. Therefore, we are not able to comment on whether management has fully addressed our comment as raised in the prior year.

WBON0001487

			Developers have access to move their own changes into production and documentation is not retained to substantiate those changes there is a risk of loss of data and application integrity due to either unauthorized, erroneous or inappropriate changeng made to the production environment.			
13	**Credence (front end) change process**	IT	During our walkthrough of user administration of the front end of Credence we noted several users with administrator rights, including some generic users (this is noted below as a separate point). These users have the access rights to create and amend reports, including those which may be relied upon for audit evidence. These users can change report design, and processing without documented request, test or approval. When users have the rights to change reports that are used by the business for reconciliation, exception reporting or other processing, there is the risk that the reports are manipulated either intentionally or accidentally.	Changes to Credence should be requested, tested and approved by the business users. Changes should be identifiable through system logs and an appropriate audit trail maintained of request, testing and approval documentation, Access to make such changes should be limited to authorised individuals.	Whilst users are able to make changes to reports they "own", those which are used for business critical processes are created globally and owned by one of the administrators. Users may be able to design their own versions of the reports but these would not be available globally, nor used for business critical processes.	Application not in audit scope for FY11. Therefore, we are not able to comment on whether management has fully addressed our comment as raised in the prior year.
14	**Credence (front end) configuration**	IT	We noted several control weakness in Credence front end user administration and security configuration:	Management should enhance password controls on the Credence web portal to the same standards applied to other	Users are not generic, but role accounts which are allocated to individuals and for which an audit trail is	Application not in audit scope for FY11. Therefore, we are not able to

WBON0001487

			1. The password configuration is not aligned with network settings or those settings required by Post Office. We noted: a. there is no minimum password length b. Password complexity rules are not applied c. users are not required to change their password d. password history is not retained e. idle session time-outs are not in place 2. There are three generic administrator accounts without specific users assigned to these accounts. One of the three accounts has not been used since April 2009. 3. The process for requesting and granting user access rights to Credence does not maintain documentation to record evidence of request or approval of access rights. 4. There is no process in place for the revocation of user access rights when a user separates from the	Post Office environments. Management should consider disabling generic administrator accounts, or assigning the accounts to specific individuals to ensure accountability over the use of the administrator accounts. Management should consider establishing user administration controls which are in-line with the processes used for other Post Office applications.	available. The correct procedure to be followed for the allocation and use of these roles is being re-emphasised. A full risk assessment of the Credence system is being undertaken later this year and this aspect will be reviewed. Although system-based credential control does not fully match POL standards, user guidelines and procedures do. The whole user management piece is due to be reviewed during the planned risk assessment.	comment on whether management has fully addressed our comment as raised in the prior year.

WBON0001487

			organisation or moves to a new role no longer requiring access rights to Credence. Without effective logical access controls there is the risk of inappropriate or unauthorised access to the Credence reports.			

From: Catherine Hamilton
Sent: 26 October 2018 14:22
To: Peter Stanley <GRO>; Michael Austin <GRO>; Ben Cooke <GRO>
Subject: FW: URGENT PLEASE- Information needed for GLO Horizon issues Trial
Importance: High

Confidential; not to be forwarded.

Hi Peter,

As you were at POL in 2011, I'm wondering if you could take a read of this and let me know if you are able to comment, and whether you think anyone else could>

Hi Michael, Ben, would you have any views on this from good practice perspective?

Hi Ben, do you know of anyone who was involved in Credence at the time?

Thanks

Catherine

WBON0001487

From: Angela Van-Den-Bogerd
Sent: 26 October 2018 12:22
To: Catherine Hamilton <GRO>; Johann Appel <GRO>
Cc: Garry Hooton <GRO>; Lucy Bremner <GRO>; Mark Underwood1 <GRO>
Subject: URGENT PLEASE- Information needed for GLO Horizon issues Trial
Importance: High

Catherine, Johann,

As part of the Post Office litigation, WBD our external lawyers are drafting our witness statements with us in response to allegations made by the other side. The one I need your help with in is respect of Jason Coyne, the Claimants' IT expert who refers to an audit document produced by E&Y in 2011 (see attached) which identified issues with the credence application, namely weak change controls within the back end of the systems allowing Logica developers (the third-party provider) to move their own uncontrolled changes into the production environment. He goes on to say that "further documentation to approve fixes and patches applied to Credence outside of the release process were lacking, therefore linking changes to issue tickets to record the original request for the bug fix was not possible".

We need to understand whether these comments are correct and whether anything changed in light of the report.

-

My expectation is that we as a business would have taken action as a result of these findings by E&Y and would have documented what that action was. I understand from speaking with Garry that we didn't have own POL internal audit function at the time as this was within the Royal Mail group structures.

Mark Hotson has already provided some information (email below) but that is about current practices rather than in 2011 following the E&Y report.

Could I ask that you both consider the initial request from Lucy (first email in chain) and provide responses from your respective areas that will help to provide an adequate response from us (POL) as part of the evidence we provide to the Court.

-

As I'm sure you'll understand this is urgent as we are on a court deadline to submit our witness statements by 4pm on 13th November but we need to get our draft statements to our Counsel early next week. So could I request that you give this your most urgent attention.

Any queries please come back to me in the first instance.

WBON0001487

Thanks,

Angela

Angela Van Den Bogerd

Business Improvement Director

1st Floor,Ty Brwydran,

Atlantic Close,Llansamlet
Swansea SA7 9FJ

GRO

Confidential Information:
This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorised review, use, disclosure or distribution is prohibited. If you are not the intended recipient please contact me by reply email and destroy all copies of the original message.

From: Mark Hotson
Sent: 25 October 2018 18:56
To: Angela Van-Den-Bogerd < GRO
Cc: Somita Yogi < GRO
Subject: Fwd: Horizon issues - witness evidence [WBDUK-AC.FID27032497]

Hi Angela,

Just picked your email exchange up with Lucy.

Please find enclosed the response that I provided her with earlier today.

Regards,

Mark

WBON0001487

Get Outlook for Android

From: Mark Hotson
Sent: Thursday, October 25, 2018 11:17:24 AM
To: Lucy Bremner
Cc: Mark Underwood1; Jonathan Gribben
Subject: RE: Horizon issues - witness evidence [WBDUK-AC.FID27032497]

Morning Lucy,

Further to the below, I have discussed the attached document, specifically items referenced "12", "13" and "14", internally and provide the following updates. These responses are based on current knowledge as those consulted were also not employed by POL at the time when the audit report was written:

Generally, since the report was written there has been:

1. A change to the IT Supplier (from: CMG Logica to: Accenture).
2. An upgrade to the application (from: Business Objects v3.1 to: v4.1).
3. A re-platform of the underlying database (from: a mix of CMG Logica locally-hosted (non-production) environment and a Fujitsu hosted (production) environment to: Microsoft Azure cloud hosting for non-production and production.

"12 - Credence (back end) change process"

- *"Developers at Logica, the third party provider of application development and support for Credence, had access rights to the production environment and the database that would permit developers to move their own changes into the production environment."*
- *"Documentation to approve fixes and patches that are applied to Credence outside of the release process does not always exist. We were advised by Logica personnel that for a sample of four changes selected evidence of approval to move into production did not exist and that it would not be possible to link the changes to problem tickets to record the original request for the fix / patch."*

All changes* are under the control of Accenture and are subject to a robust Change Management process. *These changes include: fixes – planned and emergency, project changes and security changes. Each change is subject to approval at the "CAB" (Change Approval Board)

Further to this, as the hosting is now Microsoft Azure the implementation of patches and fixes are subject to Microsoft security best practices.

WBON0001487

"13 - Credence (front end) change process"

- *"During our walkthrough of user administration of the front end of Credence we noted several users with administrator rights, including some generic users (this is noted below as a separate point). These users have the access rights to create and amend reports, including those which may be relied upon for audit evidence. These users can change report design, and processing without documented request, test or approval."*

- *"When users have the rights to change reports that are used by the business for reconciliation, exception reporting or other processing, there is the risk that the reports are manipulated either intentionally or accidentally."*

Users with administrator rights now purely carry out administrator tasks only, i.e. no reports are created or amended by users with such rights.

In addition, a Power App has been implemented which logs and controls requests for change (new and existing reports) carried out by POL personnel. Similarly, requests for changes/new reports that are assigned to Atos information Services are logged and controlled via the Atos Service Catalogue.

"14 - Credence (front end) configuration"

"We noted several control weakness in Credence front end user administration and security configuration:

1. *The password configuration is not aligned with network settings or those settings required by Post Office. We noted:*

    a. *there is no minimum password length*

    b. *Password complexity rules are not applied*

    c. *users are not required to change their password*

    d. *password history is not retained*

    e. *idle session time-outs are not in place"*

The below screenshot provides the current (as at 25/10/2018) Business Objects Central Management Console enterprise settings relating to passwords – this addresses the above:

WBON0001487

- *"There are three generic administrator accounts without specific users assigned to these accounts. One of the three accounts has not been used since April 2009."*

Only 1 full Administrator account remains which is used for administrative activities only by the POL Credence Administrator.

- *"The process for requesting and granting user access rights to Credence does not maintain documentation to record evidence of request or approval of access rights."*

This activity is now governed and controlled by the IT Service Desk. Service tickets are used to log and control requests.

- *"There is no process in place for the revocation of user access rights when a user separates from the organisation or moves to a new role no longer requiring access rights to Credence."*

Housekeeping is actively performed on a regular basis and redundant user accounts are terminated accordingly.

With regards,

Mark

WBON0001487

2017
Winner of the Global Postal Award for Customer Experience

Mark Hotson
Senior Data & Process Specialist

Data Centre of Excellence

No1 Future Walk,

West Bars,
CHESTERFIELD

Derbyshire, S49 1PF

STD: GRO

Mobile: GRO

Annual Leave Advanced Notification:

24th December 18 – 11th January 19

From: Mark Hotson
Sent: 24 October 2018 15:16
To: 'Lucy Bremner' <GRO
Cc: Mark Underwood1 <GRO>; Jonathan Gribben <GRO
GRO
Subject: RE: Horizon issues - witness evidence [WBDUK-AC.FID27032497]

Hi Lucy,

Whilst I am more than willing to try and help I wasn't working in POL in 2011!

I'll come back to you in the morning after I've had some conversations internally.

Regards,

Mark

2017 Winner of the Global Postal Award for Customer

Mark Hotson
Senior Data & Process Specialist

WBON0001487

Data Centre of Excellence

No1 Future Walk,

West Bars,
CHESTERFIELD

Derbyshire, S49 1PF

STD: GRO

Mobile: GRO

Annual Leave Advanced Notification:

24th December 18 – 11th January 19

From: Lucy Bremner [mailto: GRO
Sent: 24 October 2018 10:11
To: Mark Hotson < GRO
Cc: Mark Underwood1 < GRO >; Jonathan Gribben GRO
GRO
Subject: Horizon issues - witness evidence [WBDUK-AC.FID27032497]

Dear Mark,

As part of the Post Office litigation we are drafting witness statements in response to allegations made by the other side. I have been in contact with Paul Smith, who has pointed me in your direction in relation to one of the issues we need to respond to.

Jason Coyne, the Claimants' IT expert, refers to an audit document produced by E&Y in 2011 (see attached) which identified issues with the credence application, namely weak change controls within the back end of the systems allowing Logica developers (the third-party provider) to move their own uncontrolled changes into the production environment. He goes on to say that "further documentation to approve fixes and patches applied to Credence outside of the release process were lacking, therefore linking changes to issue tickets to record the original request for the bug fix was not possible".

We need to understand whether these comments are correct and whether anything changed in light of the report.

As we need this information urgently, can you let me know if you are the right person to answer this and if so, can we set up a call for later today/tomorrow morning to discuss?

Kind regards,

WBON0001487

Lucy

Lucy Bremner
Associate
Womble Bond Dickinson (UK) LLP

d:
m: GRO
t:
e:

Stay informed: sign up to our e-alerts

WOMBLE BOND DICKINSON

womblebonddickinson.com

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

The information in this e-mail and any attachments is confidential and may be legally privileged and protected by law. mark.hotson[GRO] only is authorised to access this e-mail and any attachments. If you are not mark.hotson[GRO], please notify lucy.bremner[GRO] as soon as possible and delete any copies. Unauthorised use, dissemination, distribution, publication or copying of this communication or attachments is prohibited and may be unlawful. Information about how we use personal data is in our Privacy Policy on our website.

Any files attached to this e-mail will have been checked by us with virus detection software before transmission. Womble Bond Dickinson (UK) LLP accepts no liability for any loss or damage which may be caused by software viruses and you should carry out your own virus checks before opening any attachment.

Content of this email which does not relate to the official business of Womble Bond Dickinson (UK) LLP, is neither given nor endorsed by it.

This email is sent by Womble Bond Dickinson (UK) LLP which is a limited liability partnership registered in England and Wales under number OC317661. Our registered office is 4 More London Riverside, London, SE1 2AU, where a list of members' names is open to inspection. We use the term partner to refer to a member of the LLP, or an employee or consultant who is of equivalent standing. Our VAT registration number is GB123393627.

Womble Bond Dickinson (UK) LLP is a member of Womble Bond Dickinson (International) Limited, which consists of independent and autonomous law firms providing services in the US, the UK, and elsewhere around the world. Each Womble Bond Dickinson entity is a separate legal entity and is not responsible for the acts or omissions of, nor can bind or obligate, another Womble Bond Dickinson entity. Womble Bond Dickinson (International) Limited does not practice law. Please see www.womblebonddickinson.com/legal notices for further details.

Womble Bond Dickinson (UK) LLP is authorised and regulated by the Solicitors Regulation Authority.