
From: Jocson, Ervin [GRO]
Sent: Wed 14/12/2011 10:11:27 AM (UTC)
To: Deaton Mike [GRO]; Phillips Edward [GRO]
Cc: Starnes, Chris [GRO]
Subject: RE: Horizon OnLine Integrity Testing: Proposal

Mike,

Thanks for confirming. We are now updating the proposal accordingly and aim to have this to you by COB today.

Ed,
Were you going to send through some words in respect to the usage & treatment & distribution of reports provided by KPMG to Fujitsu, such that we can include this in the proposal, and when we draft the Letter of Engagement we can reflect this as well to remove the requirement for hold-harmless letters?

Kind regards,
Ervin

Ervin Jocson
Director

KPMG IT Advisory
Forensics & Risk Consulting

GRO

GRO

GRO

From: Deaton Mike [GRO]
Sent: 13 December 2011 15:36
To: Jocson, Ervin
Cc: Starnes, Chris; Phillips Edward
Subject: RE: Horizon OnLine Integrity Testing: Proposal

Ervin,

In respect to point 1, we understand that audit samples may not have been exhaustive to date, but our requirements are for KPMG to highlight and such areas and caveat accordingly.

We are satisfied with the agreed approach on all other points of your response on 12th December.

On your mail of 11th December, you talk to the two options:

Option 1) Review and assess with an initial Fujitsu internal only report on 'as-is'. This gives Fujitsu the opportunity to proactively determine exposure and address issues from the findings as a restricted Fujitsu only document.

1.1) A follow-up review/test post any remediation carried out by Fujitsu over the findings. It is this

second report that you could use to issue externally, per your points below, as it would reflect the assured and remediated controls – thus providing an independent perspective on the integrity of the audit-trail for the system.

Option 2) Only Review, test and report on 'as-is'. This would not reflect any Fujitsu management action taken to address any findings.

We would appreciate both options to be put forward within your revised proposal in order we are able to address all alternatives with our stakeholders.

Regards,

Mike

Mike Deaton
Change & Operations Director
Business Operations

GRO



Please consider the environment - do you really need to print this email?

From: Jocson, Ervin **GRO**
Sent: 12 December 2011 17:01
To: Phillips Edward; Deaton Mike
Cc: Starnes, Chris
Subject: RE: Horizon OnLine Integrity Testing: Proposal

Hi Mike,

Further to my call with Ed covering the clause relating to use and distribution of the final deliverables, please find our responses to your other questions as follows:

1. Fujitsu already complies to audits on procedure, process and policy hence it would be anticipated that these would be cross referenced and effectively out of scope from this KPMG audit. Our scope is to ensure the technical assurance of transactions. However, page 6 suggest otherwise.

KPMG RESPONSE

We will cross reference to existing audits where these have taken place. We have used the wording "*Perform a detailed review of how integrity and security controls in the design of the system have been implemented.*" To indicate that we would want to review those audits and control documentation to ensure that the relevant controls required to provide effective IT General Control are present in this specific system.

To do otherwise would leave open the possibility that whilst Horizon and its component parts were part of the population audited in the previous audits, they might not have been part of the sample selected. Since our review is specifically focussed on, and limited to this one system, we would want to be sure, either via the work mentioned above, or by caveat that our work on the application was not undermined by any potential problems relating to the General Control environment.

2. Please can we clarify exactly what KPMG means by "transaction types" in the paragraph on document review on Page 12. Horizon supports a few thousand different types of transaction. However these

fall into about half a dozen broad categories and in all cases a transaction is recorded as part of a basket and the integrity and auditing is related to the overall basket structure. If the reference to transaction type, means one of these broad categories of transactions, then that is fine, but we feel it is unnecessary to investigate all types of Horizon transaction. We would expect this to be clarified as part of the “Understanding” sessions.

KPMG RESPONSE

By this we mean the broad categories, as you’ve noted.

3. The exact same process applies for every transaction type, hence we deem it unnecessary to test all transaction types. The integrity of the data in the audit trail is covered by the digital signature. Page 12 talks to understanding of different transaction types.

KPMG RESPONSE

This is similar to point 2 and we would therefore seek to test each of the “broad categories” .

4. Documentation – is available, but whether this is in the preferred KPMG format is unlikely. We are concerned that this would grant an open licence to significantly increase the cost to Fujitsu whilst we would derive little benefit to ourselves.

KPMG RESPONSE

We are able to work with a variety of different documentation formats. We would seek to utilise as much existing documentation as possible and would not wish to reinvent any wheels. Our aim to add value to what you already have as opposed to duplicating it.

With regard to addressing your concern around cost escalations, we have intentionally put stage gates in our approach, with the first occurring early in phase 1, such that if the documentation or information gathered does not provide a foundation to work with, we will work with you to identify a way forward, or in worst case scenario, jointly agree that the engagement be stopped.

5. Future proofing: would you please split this piece out as an optional extra on the basis that if your findings are merely to confirm good practice, then we might leverage little benefit from a future proofing process.

KPMG RESPONSE

We will split this out as requested.

Let me know if you are ok with the above, and we will reflect accordingly in to the updated proposal.

My best
Ervin

Ervin Jocson
Director

KPMG IT Advisory
Forensics & Risk Consulting

GRO

GRO

From: Jocson, Ervin
Sent: 12 December 2011 14:29
To: Phillips Edward; Deaton Mike
Subject: RE: Horizon OnLine Integrity Testing: Proposal

Ed,

Good to discuss, and we're on the same page and understanding regarding the reasons for the clause and use of hold harmless.

As agreed, please confirm as part of Fujitsu's statement of requirements,(that we will mirror into the proposal and engagement letter), some words covering the intended use and treatment of the reports and findings delivered by KPMG to Fujitsu for this engagement.

This can then de-risk the matter, removing the need for hold-harmless in relation to Fujitsu's distribution of the reports.

Mike,
I will have responses to your other points later today.

Cheers,
Ervin

Ervin Jocson
Director

KPMG IT Advisory
Forensics & Risk Consulting

GRO

GRO

From: Phillips Edward
Sent: 12 December 2011 12:41
To: Jocson, Ervin; Deaton Mike
Subject: RE: Horizon OnLine Integrity Testing: Proposal

GRO

Ervin
GRO before 1.30 would be best. Thanks.
Ed

From: Jocson, Ervin

GRO

Sent: 12 December 2011 12:40
To: Deaton Mike; Phillips Edward
Subject: RE: Horizon OnLine Integrity Testing: Proposal

Hi Mike,

I'll get your other points reviewed by my team.

Hi Ed,

I can make anytime 1-2:30pm, or anytime after 4pm.

What is the best number to get you on?

Cheers,
Ervin

Ervin Jocson
Director

KPMG IT Advisory
Forensics & Risk Consulting

The logo consists of the letters "GRO" in a large, bold, black, sans-serif font. The letters are centered within a rectangular frame defined by a dashed border.

From: Deaton Mike
Sent: 12 December 2011 11:42
To: Jocson, Ervin
Cc: Phillips Edward
Subject: RE: Horizon OnLine Integrity Testing: Proposal

GRO

Ervin,

Thanks for the reply and clarification.

Your 1.1) below appears contradictory with your proposal

"At the conclusion of Phase two, Fujitsu will have a comprehensive report to be used only for its own internal risk and commercial compliance assessment"

,but this may be my naivety in your latter comment below regarding distribution.

I would like Ed to bottom out on this point with you please. If it is possible to get a call today pre 13:30 or 15:00-16:00, that would be great.

The other areas to which we require clarity, and any subsequent amendment to your proposal, are listed below:

1. Fujitsu already complies to audits on procedure, process and policy hence it would be anticipated that these would be cross referenced and effectively out of scope from this KPMG audit. Our scope is to ensure the technical assurance of transactions. However, page 6 suggest otherwise.
2. Please can we clarify exactly what KPMG means by “transaction types” in the paragraph on document review on Page 12. Horizon supports a few thousand different types of transaction. However these fall into about half a dozen broad categories and in all cases a transaction is recorded as part of a basket and the integrity and auditing is related to the overall basket structure. If the reference to transaction type, means one of these broad categories of transactions, then that is fine, but we feel it is unnecessary to investigate all types of Horizon transaction. We would expect this to be clarified as part of the “Understanding” sessions.
3. The exact same process applies for every transaction type, hence we deem it unnecessary to test all transaction types. The integrity of the data in the audit trail is covered by the digital signature. Page 12 talks to understanding of different transaction types.
4. Documentation – is available, but whether this is in the preferred KPMG format is unlikely. We are concerned that this would grant an open licence to significantly increase the cost to Fujitsu whilst we would derive little benefit to ourselves.
5. Future proofing: would you please split this piece out as an optional extra on the basis that if your findings are merely to confirm good practice, then we might leverage little benefit from a future proofing process.

On these 5 areas, it would be useful to get a quick position/understanding from you, if possible today. We may need to set up a session with our respective teams to narrow down and can do this in coming days.

Regards,

Mike

Mike Deaton
Change & Operations Director
Business Operations

Fujitsu

GRO



Please consider the environment - do you really need to print this email?

From: Jocson, Ervin

GRO

Sent: 11 December 2011 23:12
To: Deaton Mike
Cc: Phillips Edward
Subject: RE: Horizon OnLine Integrity Testing: Proposal

Hi Mike,

The reason for this clause is to support Fujitsu's requirement to undertake a proactive 'internal' risk assessment, whereby the report is used initially by Fujitsu to determine and inform its legal position, and act on any gaps, and perform remediation from the findings.

Stage 1 & 2 effectively enable Fujitsu to assert the existence of controls, and for KPMG to then test and validate these assertions based on agreed-upon procedures.

As discussed at the scoping meeting there are two options, which we understand option 1 being the Fujitsu requirement:

Option 1) Review and assess with an initial Fujitsu internal only report on 'as-is'. This gives Fujitsu the opportunity to proactively determine exposure and address issues from the findings as a restricted Fujitsu only document.

1.1) A follow-up review/test post any remediation carried out by Fujitsu over the findings. It is this second report that you could use to issue externally, per your points below, as it would reflect the assured and remediated controls – thus providing an independent perspective on the integrity of the audit-trail for the system.

Option 2) Only Review, test and report on 'as-is'. This would not reflect any Fujitsu management action taken to address any findings.

For both options, should Fujitsu want to waiver its legal privileges regarding the distribution of the deliverable reports externally and to other parties, this will be subject to agreement of 'hold harmless' letters with KPMG. This is because Fujitsu's requirement in this case is bespoke compared to a SAS70 or ISA3042 equivalent certification and audit opinion, which can typically be freely distributed by Fujitsu.

Let me know what time suits you to discuss on Monday.

Regards,
Ervin

Ervin Jocson
Director

KPMG IT Advisory
Forensics & Risk Consulting

A large, bold, black 'GRO' logo is centered within a dashed rectangular border.A smaller, bold, black 'GRO' logo is positioned to the right of the 'From' field in the email footer.

From: Deaton Mike
Sent: 09 December 2011 11:51

To: Jocson, Ervin
Cc: Phillips Edward
Subject: RE: Horizon OnLine Integrity Testing: Proposal

Ervin,

As previously mentioned I aim to come back to you early next week in respect to our points on your proposal having briefed my stakeholders.

A key area noted, however, is the restriction on page 3 under heading "Stage Two" that "...Fujitsu will have a comprehensive report to be used only for its own internal risk and commercial compliance assessment. "

We are primarily commissioning this report in order to inform our legal team, as discussed. However, if we later choose to waive legal privilege on this document, we would be expect to be able to produce it freely in to other auditors, Post Office, in disputes (either between us and Post Office, or where we are supporting Post Office in defending the integrity of its systems). We appreciate that you will not be expert witnesses, but that is a separate issue to not being able to use this document for any external purpose. We therefore need to understand whether this is intended to be a restriction on use of the report, and if so, we need this restriction to be relaxed and will need to discuss with you how that can be achieved.

Could we please set up a quick call on Monday morning to discuss the intent of this clause?

Thank you.

GRO



Please consider the environment - do you really need to print this email?

From: Jocson, Ervin
Sent: 04 December 2011 14:06
To: Deaton Mike
Subject: RE: Horizon OnLine Integrity Testing: Proposal

GRO

Hi Mike,

Thanks for the update.

As you would have noted, we have issued the proposal in 'draft for discussion/comment' to provide you an opportunity to refine the scope/deliverables if needed.

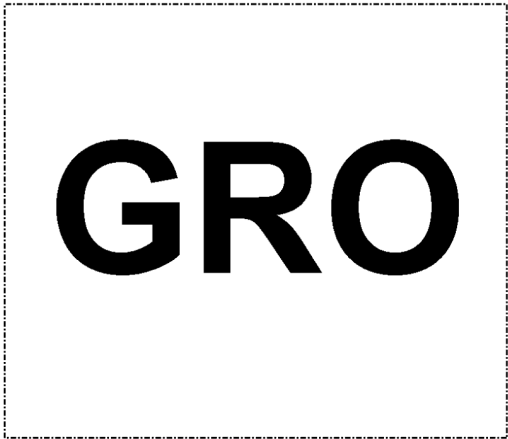
We've scoped a multi-dimension approach to getting assurance and comfort over the integrity of the data & audit trail of the system, based on our

understanding from our discussions and the updated scoping/ToR document.

We look forward to your approval or feedback in the coming week.

My best,
Ervin

Ervin Jocson
Director

A large rectangular box with a dashed border containing the letters "GRO" in a bold, black, sans-serif font.

Please consider the environment before printing this e-mail

Latest KPMG insights and research

Fraud Barometer January 2011: Click [here](#) to read KPMG's latest Fraud Barometer results.

Consumers and Convergence IV: Read KPMG's latest research into internet and mobile trends. Visit www.KPMG.co.uk/convergence

From: Deaton Mike

GRO

Sent: 02 December 2011 18:36

To: Jocson, Ervin

Subject: RE: Horizon OnLine Integrity Testing: Proposal

Thanks, Ervin,

I am trying to organise a meeting with my team next week prior to making recommendations to my key stakeholders.

I aim to be in touch within the week.

Regards,

Mike

Mike Deaton
Change & Operations Director
Business Operations

Fujitsu

A rectangular box with a dashed border containing the letters "GRO" in a bold, black, sans-serif font.

Email
Web

GRO



Please consider the environment - do you really need to print this email?

GRO

From: Jocson, Ervin
Sent: 01 December 2011 16:59
To: Deaton Mike
Cc: Starnes, Chris
Subject: RE: Horizon OnLine Integrity Testing: Proposal

Hi Mike,

As committed please find attached our draft proposal for your comment/approval, which is in response to your revised ToR scope document issued to us on the 25th Nov 2011.

Our approach factors in your feedback below.

Please contact me should you have any questions.

My best,
Ervin

Ervin Jocson
Director

KPMG IT Advisory
Forensics & Risk Consulting

GRO

Please consider the environment before printing this e-mail

Latest KPMG insights and research

Fraud Barometer January 2011: Click [here](#) to read KPMG's latest Fraud Barometer results.

Consumers and Convergence IV: Read KPMG's latest research into internet and mobile trends. Visit www.KPMG.co.uk/convergence

From: Deaton Mike
Sent: 01 December 2011 14:57
To: Jocson, Ervin
Cc: Rahman, Mohammed R (UK); Starnes, Chris; Edge, Lee; Morjaria, Nishad; Howard Ian; Jenkins Gareth GI
Subject: RE: Horizon OnLine Integrity Testing

GRO

Ervin,

Apologies for the delay in getting back to you.

We need KPMG to define a set of scenarios taking enough to demonstrate robustness of the overall process. This may be more than the scenarios that we have defined, but need KPMG to make this recommendation

The objective is to audit the integrity of the overall basket process. Transaction audits should not be necessary to achieve this.

Regards,

Mike

Mike Deaton
Change & Operations Director
Business Operations

A large, bold, black 'GRO' logo is centered within a dashed rectangular border.A smaller, bold, black 'GRO' logo is positioned to the right of the main logo, also within a dashed rectangular border.

From: Jocson, Ervin

Sent: 28 November 2011 10:14

To: Deaton Mike

Cc: Rahman, Mohammed R (UK); Starnes, Chris; Edge, Lee; Morjaria, Nishad

Subject: RE: Horizon OnLine Integrity Testing

Hi Mike,

I hope you had a nice weekend. Just as an update – We're aiming to get the proposal back to you by this Thursday for your review.

We have a few questions in relation to your updated scoping document:

- Section 1.2 – Scope. In shaping our approach, we will define an agreed-upon procedure for the audit. To help guide and size the audit, will Fujitsu have a minimum or maximum number of prescribed transaction types to be tested?
- Section 1.3 – Deliverables: For clarity, Fujitsu have specified the delivery of an 'audit report' that may be

submitted in court to demonstrate adequacy of the controls in place. As discussed at our scoping meeting, we can provide litigation support, particularly of the nature in the scope of your requirements. However as external auditors we are restricted from providing expert witness services, particularly where there is a quantum aspect that results in us actually self auditing such material values through the external audit.

- Section 3.0 – for clarity, we interpret these scenarios as the ‘test scenarios’ that may occur stand-alone or in combinations, in which transaction audits need to be validated against. Is this correct?

In our proposal response we will outline an approach in terms of two iterations of deliverables. This will enable us to expedite the initial findings audit report for Fujitsu ‘ONLY’ review and action. With the second iteration reflecting your comments/feedback that will be subject to final risk review by KPMG such that the final release can be relied-upon.

Many thanks,
Ervin

Ervin Jocson
Director

KPMG IT Advisory
Forensics & Risk Consulting

The logo consists of the letters 'GRO' in a large, bold, black, sans-serif font. The letters are centered within a square frame defined by a dashed line.

Please consider the environment before printing this e-mail

Latest KPMG insights and research

Fraud Barometer January 2011: Click [here](#) to read KPMG's latest Fraud Barometer results.

Consumers and Convergence IV: Read KPMG's latest research into internet and mobile trends. Visit www.KPMG.co.uk/convergence

From: Deaton Mike

GRO

Sent: 25 November 2011 09:51

To: Jocson, Ervin

Subject: Horizon OnLine Integrity Testing

Ervin,

Please find attached our revised scoping document for your review. I trust this covers everything you need, but please call out if you believe there is anything missing.

I have asked Tim Healy to organise countersignature to the NDA and will have this across to you early next week.

Do you have any view of timescales as to when you think you might provide your proposal,

Regards,

Mike Deaton
Change & Operations Director
Business Operations

GRO



Please consider the environment - do you really need to print this email?

This email has been sent from KPMG LLP, a UK limited liability partnership (which is a subsidiary of KPMG Europe LLP), from KPMG Europe LLP, from one of the companies within KPMG LLPs control (which include KPMG Audit Plc, KPMG United Kingdom Plc and KPMG UK Limited) or from KPMG Resource Centre Private Limited, together "KPMG". KPMG Europe LLP does not provide services to clients. None of KPMG Europe LLPs subsidiaries have any authority to obligate or bind KPMG Europe LLP. This email is confidential and may be legally privileged. It is intended solely for the addressee. Access to this email by anyone else is

unauthorised. If you are not the addressee or an intended recipient or have not agreed with us the terms on which you are receiving this email any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on the contents of this email or its attachments, is at your own risk, prohibited and may be unlawful, and to the fullest extent permitted by law KPMG accepts no responsibility or liability to you.

When addressed to our clients any opinions or advice contained in this email or its attachments are subject to the terms and conditions expressed in the governing KPMG client engagement letter. Anything in this email or its attachments which does not relate to KPMG's official business is neither given nor endorsed by KPMG.

KPMG Europe LLP, registered in England
No OC324045
Registered office: 15 Canada Square,
London, E14 5GL

KPMG United Kingdom PLC, registered in
England No 03513178
Registered office: 15 Canada Square,
London, E14 5GL

KPMG UK Limited, registered in England
No 3580549
Registered office: 15 Canada Square,
London, E14 5GL

KPMG LLP, registered in England No
OC301540
Registered office: 15 Canada Square,
London, E14 5GL

KPMG Audit Plc, registered in England
No 3110745
Registered office: 15 Canada Square,
London, E14 5GL

Unless otherwise stated, this email has been sent from

Fujitsu Services Limited, from Fujitsu (FTS) Limited, or from Fujitsu Telecommunications Europe Limited, together "Fujitsu".

This email is only for the use of its intended recipient. Its contents are subject to a duty of confidence and may be privileged. Fujitsu does not guarantee that this email has not been intercepted and amended or that it is virus-free.

Fujitsu Services Limited, registered in England No 96056, registered office 22 Baker Street, London W1U 3BW.

Fujitsu (FTS) Limited, registered in England No 03808613, registered office 22 Baker Street, London W1U 3BW.

Fujitsu Telecommunications Europe Limited, registered in England No 2548187, registered office Solihull Parkway, Birmingham Business Park, Birmingham, B37 7YU.

Unless otherwise stated, this email has been sent from Fujitsu Services Limited, from Fujitsu (FTS) Limited, or from Fujitsu Telecommunications Europe Limited, together "Fujitsu".

This email is only for the use of its intended recipient. Its contents are subject to a duty of confidence and may be privileged. Fujitsu does not guarantee that this email has not been intercepted and amended or that it is virus-free.

Fujitsu Services Limited, registered in England No 96056, registered office 22 Baker Street, London W1U 3BW.

Fujitsu (FTS) Limited, registered in England No 03808613, registered office 22 Baker Street, London W1U 3BW.

Fujitsu Telecommunications Europe Limited, registered in England No 2548187, registered office Solihull Parkway, Birmingham Business Park, Birmingham, B37 7YU.

Unless otherwise stated, this email has been sent from Fujitsu Services Limited, from Fujitsu (FTS) Limited, or from Fujitsu Telecommunications Europe Limited, together "Fujitsu".

This email is only for the use of its intended recipient. Its contents are subject to a duty of confidence and may be privileged. Fujitsu does not guarantee that this email has not been intercepted and amended or that it is virus-free.

Fujitsu Services Limited, registered in England No 96056, registered office 22 Baker Street, London W1U 3BW.

Fujitsu (FTS) Limited, registered in England No 03808613, registered

office 22 Baker Street, London W1U 3BW.

Fujitsu Telecommunications Europe Limited, registered in England No 2548187, registered office Solihull Parkway, Birmingham Business Park, Birmingham, B37 7YU.

Unless otherwise stated, this email has been sent from Fujitsu Services Limited, from Fujitsu (FTS) Limited, or from Fujitsu Telecommunications Europe Limited, together "Fujitsu".

This email is only for the use of its intended recipient. Its contents are subject to a duty of confidence and may be privileged. Fujitsu does not guarantee that this email has not been intercepted and amended or that it is virus-free.

Fujitsu Services Limited, registered in England No 96056, registered office 22 Baker Street, London W1U 3BW.

Fujitsu (FTS) Limited, registered in England No 03808613, registered office 22 Baker Street, London W1U 3BW.

Fujitsu Telecommunications Europe Limited, registered in England No 2548187, registered office Solihull Parkway, Birmingham Business Park, Birmingham, B37 7YU.

Unless otherwise stated, this email has been sent from Fujitsu Services Limited, from Fujitsu (FTS) Limited, or from Fujitsu Telecommunications Europe Limited, together "Fujitsu".

This email is only for the use of its intended recipient. Its contents are subject to a duty of confidence and may be privileged. Fujitsu does not guarantee that this email has not been intercepted and amended or that it is virus-free.

Fujitsu Services Limited, registered in England No 96056, registered office 22 Baker Street, London W1U 3BW.

Fujitsu (FTS) Limited, registered in England No 03808613, registered office 22 Baker Street, London W1U 3BW.

Fujitsu Telecommunications Europe Limited, registered in England No 2548187, registered office Solihull Parkway, Birmingham Business Park, Birmingham, B37 7YU.

Unless otherwise stated, this email has been sent from Fujitsu Services Limited, from Fujitsu (FTS) Limited, or from Fujitsu Telecommunications Europe Limited, together "Fujitsu".

This email is only for the use of its intended recipient. Its contents are subject to a duty of confidence and may be privileged. Fujitsu does not guarantee that this email has not been intercepted and amended or that it is virus-free.

Fujitsu Services Limited, registered in England No 96056, registered office 22 Baker Street, London W1U 3BW.

Fujitsu (FTS) Limited, registered in England No 03808613, registered office 22 Baker Street, London W1U 3BW.

Fujitsu Telecommunications Europe Limited, registered in England No 2548187, registered office

Solihull Parkway, Birmingham Business Park, Birmingham, B37 7YU.