To: Andy J Jones[GRO]; Don M Burgess[GRO]
Cc: Howard Ian[GRO]; Arnold Mark[GRO]; Davidson James[GRO]; Long Stephen[GRO]; Apte Amit[GRO]; Beresford Peter[GRO]
From: Membery Bill[/O=EXCHANGE/OU=ADMINGROUP1/CN=RECIPIENTS/CN=MEMBERYW]
Sent: Wed 5/18/2011 11:23:22 AM (UTC)
Subject: FW: Management Letter response

Hi Andy

You asked that we formally respond to the Draft Ernst and Young Management Letter Mark and I have undertaken a review of each of their findings and below are our responses. One key point we do feel needs addressing though is the classification of these and how this has been arrived at as Ernst and Young classifications may not be the same as PO Ltd's or Fujitsu's view.

1. Item 1 - Improve Governance of outsourcing Application Management – High. Is according to Don being rewritten we agree to respond when we see the revised version

2. Item 2 - strengthen the password parameters– Low. The Password policy in SVM/SEC/POL/0003 RMG BU Security Policy we need to amend section 11.2.5 in the next review of the policy, provided agreement is obtained from Architects, and if there is a reason this cannot be met in any systems document the reason as a risk. – Action Ian Howard, Amit Apte

   Also we will send out a Cascade to all users especially SAP and Linux and remind them of the policy and guidelines . Initialise a BAU monthly report concerning passwords to provide assurance to PO Ltd that this is being managed ongoing. - action Ian Howard and Donna Munro

3. Item 3 Review of Privileged Access– High. A project has been established by Stephen Long to review all user management and is being led Ian Howard. – action Ian Howard all areas of the account.

   Also a cascade to all areas of the account to advise them of the process for new joiners, movers and leavers – action Donna Munro
   Regular BAU reports of Privileged Access abuse to provide PO ltd with the assurances they require – action Ian Howard, Donna Munro

4. Item 4 - Implement Periodic User Access Reviews and Monitoring Controls – Medium. A project has been established by Stephen Long to review all user management areas and is being led Ian Howard. – action Ian Howard all areas of the account.

   Review User Management Process SVM/SEC/PRO/00012 RMGA User Management Process Guide and SVM/SEC/PRO/0006 RMGA Application for Access to the Live Network to ensure that the requirements are documented. – Action Ian Howard and Donna Munro

   Quarterly BAU Assurance reports to PO Ltd concerning reviews that have occurred across the account – Action Ian Howard, Donna Munro

   Senior Management to include responsibilities on all Line managers/Assignment Managers to review rights of their staff and their appropriateness every quarter – Action Senior Management Team

5. Item 5 – Segregation of duties within the Manage Change Process – High A project has been established by Stephen Long to review all user management areas and is being led Ian Howard. – action Ian Howard all areas of the account.

   A clear segregation of duties guideline is required for Senior Management and Line managers/Assignment managers to ensure that development and test are clearly separated from live in all technological and staff areas. If it is not possible to do this then risks identifying why this is not the case should be documented and assessed. - Action Ian Howard, Donna Munro

   Third parties including other parts of Fujitsu outside of RMG BU also should have obligations upon them to ensure the segregation of Development and Test systems, a review of OLA's, SLA's , NDA's and Contractual agreements is required to ensure this. – Action Ian Howard, Peter Beresford, Marc Daniel Lamaziere, Tony Atkinson, Peter Thompson.

Assurance given to PO Ltd as part of the regular BAU reports that this is occurring – Action Ian Howard, Donna Munro

6. Item 6- Strengthen the User Administration Process – Medium A project has been established by Stephen Long to review all user management areas and is being led Ian Howard. – action Ian Howard all areas of the account.

   Review User Management Process SVM/SEC/PRO/00012 RMGA User Management Process Guide and SVM/SEC/PRO/0006 RMGA Application for Access to the live network to ensure that the requirements are documented. – Action Ian Howard and Donna Munro.

   Third parties including other parts of Fujitsu outside of RMG BU also should have obligations upon them to ensure user administration is in place, a review of OLA's, SLA's , NDA's and Contractual agreements is required to ensure this. – Action Ian Howard, Peter Beresford, Marc Daniel Lamaziere, Tony Atkinson, Peter Thompson.

   Quarterly BAU Assurance reports to PO Ltd concerning reviews that have occurred across the account – Action Ian Howard, Donna Munro

7. Item 7- Improvements to Logical Security Settings – [redacted] A technical review of all applications, operating systems and access and authentication tools is to be undertaken. – Amit Apte to manage

   A periodic scan of passwords is to be made as part of a regular Pen Test Exercise once agreed as part of the BAU discussions with Fujitsu. – Ian Howard

8. Item 8 - Strengthen the Change Management Process – [redacted] A central location for PO Ltd approvals for change is to be established, which is accessible to all relevant staff and is to be applied throughout the development, testing and release process to evidence PO ltd approval at each stage. – Sarah Bull & Alan Flack

9. Item 9 -Improvements to the Problem and Incident Management Process – [redacted] – Agreement of the classification and timescales for the identifications, resolution, review and analyses of incidents and this to be documented in a review of SVM/SDM/PRO/0001 and SVM/SDM/PRO/0018 Incident Management Processes – Salawu Saheed, Tony Atkinson

10. Item 10 - Review of Generic privileged accounts – Medium – Review of all non human accounts and privileges – Amit Apte

If we do not want to go into so much depth then a generic one we are looking into these and will respond on receipt of the formal report gives us time to start fixing.

Kind Regards

Bill Membery
Quality Compliance and Risk Manager
RMGA

Fujitsu Services
Unit 1- 4
Raglan Court
Clayton Road
Risley
Warrington
Cheshire
WA3 6SZ

Mobile External GRO
Mobile Internal
E-mail: **bill.membery** GRO
Web: http://uk.fujitsu.com

Fujitsu Services Limited, Registered in England no 96056, Registered Office: 22 Baker Street, London W1U 3BW

This e-mail 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 e-mail has not been intercepted and amended or that it is virus-free.

From: Membery Bill
Sent: 16 May 2011 09:17
To: Arnold Mark; Howard Ian
Cc: Davidson James; Long Stephen
Subject: FW: Management Letter response

As you can see we have been asked by PO Ltd to come back with some responses to the items defined in Ernst and Young's Draft summary report see attached.

My view is as follows, however this would need to be agreed by the management team and also scheduled into everyone's workload with timescales agreed before any commitments to PO Ltd:

11. Item 1 over governance outsourcing – [redacted]. Is according to Don being rewritten we agree to respond when we see the revised version

12. Item 2 regards amending – [redacted]. The Password policy in SVM/SEC/POL/0003 RMG BU Security Policy we need to amend section 11.2.5 in the next review of the policy, provided agreement is obtained from Architects, and if there is a reason this cannot be met in any systems document the reason as a risk. – Action Ian Howard, Amit Apte

    Also send out a Cascade to all users especially SAP and Linux and remind them of the policy and guidelines . Initialise a BAU monthly report concerning passwords to provide assurance to PO Ltd that this is being managed ongoing. - action Ian Howard and Donna Munro

13. Item 3 regards Privileged Access Review – [redacted]. A project has been established by Stephen Long to review all User management and is being led Ian Howard. – action Ian Howard all areas of the account.

    Also cascade to all areas of the account to advise them of the process for new joiners, movers and leavers – action Donna Munro
    Regular BAU reports of Privileged Access abuse to provide PO ltd with the assurances they require – action Ian Howard, Donna Munro

14. Item 4 Implement periodic reviews user access reviews and monitoring controls – Medium. A project has been established by Stephen Long to review all User management areas and is being led Ian Howard. – action Ian Howard all areas of the account.

    Review User management Process SVM/SEC/PRO/00012 RMGA User Management Process Guide and SVM/SEC/PRO/0006 RMGA Application for Access to the live network to ensure that the requirements are documented. – Action Ian Howard and Donna Munro

    Quarterly BAU Assurance reports to PO Ltd concerning reviews that have occurred across the account – Action Ian Howard, Donna Munro

    Senior management to include responsibilities on all Line managers, Assignment managers to review rights of their staff and their appropriateness every quarter – Action Senior management Team

15. Item 5 – Segregation of duties within managed change process – [redacted] A project has been established by Stephen Long to review all User management areas and is being led Ian Howard. – action Ian Howard all areas of the account.

    A clear segregation of duties guideline is required for Senior Management and Line managers to ensure that development and test are clearly separated from live in all technological and staff areas. If it is not possible to do this then risks identifying why this is not the case should be documented and assessed. - Action Ian Howard, Donna Munro

    Third parties including other parts of Fujitsu outside of RMG BU also should have obligations upon them to ensure the segregation of Development and Test systems, a review of OLA's, SLA's , NDA's and Contractual agreements is required to ensure this. – Action Ian Howard, Peter Beresford, Marc Daniel Lamaziere, Tony Atkinson, Peter Thompson.

    Assurance given to PO Ltd as part of the regular BAU reports that this is occurring – Action Ian Howard, Donna Munro

16. Strengthen the user administration Process – Medium A project has been established by Stephen Long to review all User management areas and is being led Ian Howard. – action Ian Howard all areas of the account.

    Review User management Process SVM/SEC/PRO/00012 RMGA User Management Process Guide and SVM/SEC/PRO/0006 RMGA Application for Access to the live network to ensure that the requirements are documented. – Action Ian Howard and Donna Munro.

    Third parties including other parts of Fujitsu outside of RMG BU also should have obligations upon them to ensure user administration is in place, a review of OLA's, SLA's , NDA's and Contractual agreements is required to ensure this. – Action Ian Howard, Peter Beresford, Marc Daniel Lamaziere, Tony Atkinson, Peter Thompson.

    Quarterly BAU Assurance reports to PO Ltd concerning reviews that have occurred across the account – Action Ian Howard, Donna Munro

17. Improvements to logical security settings – [redacted] A Technical review of all applications, operating systems and access and authentication tools is to be undertaken. – Amit Apte to manage

    A periodic scan of these passwords to be made as part of a regular pen test exercise. – Ian Howard

18. Strengthen the Change management process – [redacted] A central location for PO Ltd approvals for change is to be established, which is accessible to all relevant staff and is to be applied throughout the development, testing and release process to evidence PO ltd approval at each stage. – Sarah Bull & Alan Flack

19. Improvements to the problem and Incident management process – [redacted] – Agreement of the classification and timescales for the identifications, resolution, review and analyses of incidents and this to be documented in a review of SVM/SDM/PRO/0001 and SVM/SDM/PRO/0018 Incident Management Processes – Salawu Saheed, Tony Atkinson

20. Review of Generic privileged accounts – Medium – Review of all non human accounts and privileges – Amit Apte

If we do not want to go into so much depth then a generic one we are looking into these and will respond on receipt of the formal report gives us time to start fixing.

Kind Regards

Bill Membery
Quality Compliance and Risk Manager
RMGA

Fujitsu Services
Unit 1- 4
Raglan Court
Clayton Road
Risley
Warrington
Cheshire
WA3 6SZ

Mobile External GRO
Mobile Internal
E-mail: bill.membery GRO
Web: http://uk.fujitsu.com

Fujitsu Services Limited, Registered in England no 96056, Registered Office: 22 Baker Street, London W1U 3BW

This e-mail 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 e-mail has not been intercepted and amended or that it is virus-free.

From: Andy J Jones GRO
Sent: 11 May 2011 15:48
To: Membery Bill

Cc: Don M Burgess
Subject: Management Letter response

Bill

Just been speaking to E&Y. They have to report to the Audit Committee at the back end of next week and they have asked for the responses to the 10 recommendations. Now I reminded them that you had already stated that you couldn't start this work until the 9th May due to leave / work pressures etc. but I think it would be prudent to make some statement against the individual recommendations even if it is ' No concrete plan as yet, we are in the process of developing our plan of action.' Or some such phrase. It may well be that you have progressed a number of these to be able to state something more positive, but can you look to get a response against each 10 recommendations by the middle of next week (18th May), so we can agree this before its submitted. I think a response, even if it is to say where we are, is better than none and gives more comfort.

As for the re-write that was worked up with Don and submitted to E&Y, I can't say for a fact, but I believe they have removed the whole summary part but left the rest, which would be the 10 recommendations. I'll let you know more when I do.

Regards

Andy

Andy J Jones
Quality & Standards Manager
IT & Change- Post Office Ltd
148 Old Street LONDON EC1V 9HQ
Tel (GRO or GRO
Mob or
Email andy.j.jones GRO k