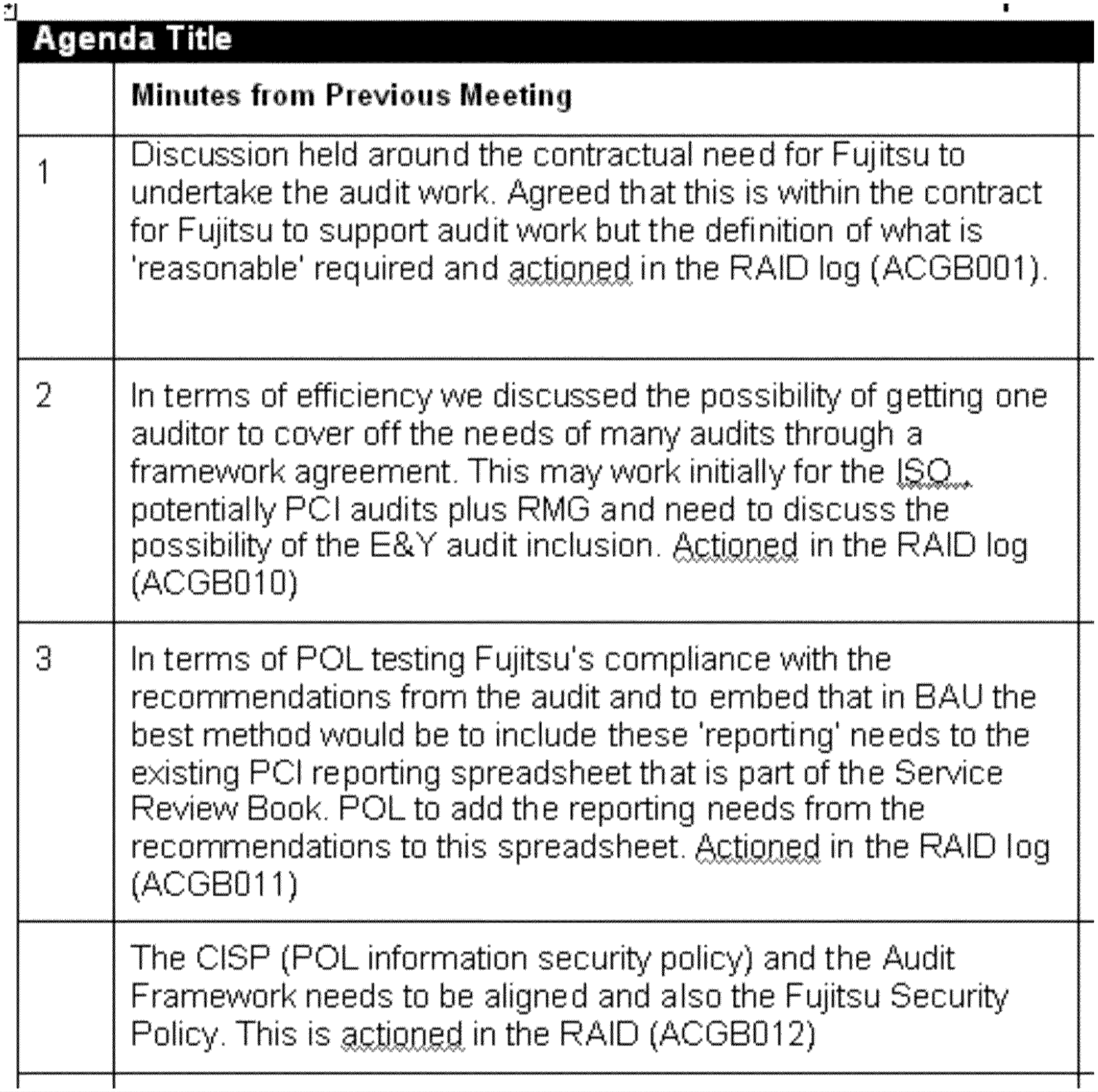
Audit Steering Group

September 22nd 2011

Agenda

1. Confirm previous minutes
2. Status update of E&Y 2011 findings resolution activities
3. Update on preparation for 2012 E&Y audit
4. Progress on consolidated Frameworks approach
5. RAID log actions update
6. RAID log risks update
7. AOB



Agenda Title	
	Minutes from Previous Meeting
1	Discussion held around the contractual need for Fujitsu to undertake the audit work. Agreed that this is within the contract for Fujitsu to support audit work but the definition of what is 'reasonable' required and actioned in the RAID log (ACGB001).
2	In terms of efficiency we discussed the possibility of getting one auditor to cover off the needs of many audits through a framework agreement. This may work initially for the ISO , potentially PCI audits plus RMG and need to discuss the possibility of the E&Y audit inclusion. Actioned in the RAID log (ACGB010)
3	In terms of POL testing Fujitsu's compliance with the recommendations from the audit and to embed that in BAU the best method would be to include these 'reporting' needs to the existing PCI reporting spreadsheet that is part of the Service Review Book. POL to add the reporting needs from the recommendations to this spreadsheet. Actioned in the RAID log (ACGB011)
	The CISP (POL information security policy) and the Audit Framework needs to be aligned and also the Fujitsu Security Policy. This is actioned in the RAID (ACGB012)

Status update 2011 findings

1. High	Improve governance of outsourcing application management as POL is responsible for the governance, risk and control framework over business critical systems and needs to have assurance over their design and operating effectiveness.	•This will be resolved by a number of activities. The following two points represent progress against the E&Y findings. •A set of BAU Review Reports are being defined by PO Ltd for Fujitsu to report against to monitor the findings. These will be our controls, reported periodically, against the user administration controls. F/C 31st October for completion and inclusion in the security review board (BAU). •An Audit Steering Group has been established within POL (Fujitsu represented) and has now met on three occasions (monthly). **(Complete)** •The next points are strategic actions for the longer term approach. •Additionally, is to incorporate where possible the IT General Controls required by E&Y into an audit framework solution along side the existing framework for ISO 27001, 20000 & 9000. PCI and LINK. This will bring much more efficiency to the audit process for all parties. This is a longer term initiative as part of a strategic plan. •POL and Fujitsu will determine the end to end process for change and identify the risk areas and controls we have in those areas. This will be utilised initially by the Ernst & Young auditors but also maintained thereafter for control purposes. This again is a longer term initiative for the strategic direction. •Finally, and not part of the E&Y findings, there is a corporate dashboard being developed between POL and Fujitsu that is currently with POL for views.	On target for completion by end October

Item 2

2. High	Segregation of duties within the change management process needs to be improved. The logical and organisational controls need to be in place to separate the development and migration of changes.	•This is part of the Overall review of User Management and Fujitsu are on target with the Project Plan. Including in this is the backend SAP applications. Active Directory is included here with the exception of TACACS+ for networks which is a separate service improvement programme. F/C 31st October 2011 •A register of all users on the POL account has been created and created into an access database. **(Complete)** •The process for administering this process is out for review within Fujitsu and once signed off will be cascaded through the POL account. F/C 31st October 2011 •The Change Management system has been updated and now includes SAP changes. In addition PO Ltd agrees Operational Changes as part of BAU **(Complete)** •A set of BAU Review Reports are being defined by PO Ltd for Fujitsu to report against to monitor the findings. These will be our controls, reported periodically, against the user administration controls. F/C 31st October 2011	[redacted]

Items 3 & 4

3. High	Strengthen the change management process to ensure that all programme changes are appropriately authorised, tested and approved prior to implementation.	•**Complete** for Fujitsu •The Change Management system has been updated to include PO Ltd agreement to Operational Changes. An Internal Share Point system is now in place for this area within Fujitsu. **(Complete)** •POL has implemented a solution to centralise the approval for all changes. **(Complete)** •A Rough Order of Magnitude (ROM) process has been introduced by Business Change and regular Business Change meetings are held with PO Ltd. **(Complete)** •POL need to test that this remedial work is appropriate. This will be performed through the RMG audit forecast last week October 2011. •POL is reviewing how we can test maintenance and fixes. The review is likely to require dedicated resource that will be part of a longer term initiative. Review F/C mid October	**Complete** for Fujitsu POL review of test still under consideration Requires testing to confirm appropriateness
4. High	Review of privileged access to IT functions including access to user administration functionality across Horizon on-line and POLSAP	•This is part of the Overall review of User Management and Fujitsu are on target with the Project Plan. Including in this is the backend SAP applications. Active Directory is included here with the exception of TACACS+ for networks which is a separate service improvement programme. F/C 31st October 2011 •A set of BAU Review Reports are being defined by PO Ltd for Fujitsu to report against to monitor the findings. These will be our controls, reported periodically, against the user administration controls. F/C 31st October 2011 •The processes for the management of SAP Accounts in cash centres has been implemented by POL **(Complete)**	On target for completion by end October

Items 5 & 6

5. Medium	Implement periodic user access reviews and monitoring controls for Horizon on-line and POLSAP to determine that user access is appropriately granted.	•This is part of the Overall review of User Management and Fujitsu are on target with the Project Plan. Including in this is the backend SAP applications. Active Directory is included here with the exception of TACACS+ for networks which is a separate service improvement programme. F/C 31st October 2011 •The process for administering this process is out for review within Fujitsu and once signed off will be cascaded through the POL account. F/C 31st October 2011 •A set of BAU Review Reports are being defined by PO Ltd for Fujitsu to report against to monitor the findings. These will be our controls, reported periodically, against the user administration controls. F/C 31st October 2011 •The processes for the management of SAP Accounts in cash centres is in the process of being implemented by POL **(Complete 09/09/11)**	On target for completion by end October The POL action regarding management control of SAP users now complete
6.Medium	Strengthen the user administration process for the granting, modification and removal for POLSAP and the authorisation for modified users in Horizon on-line	•This is part of the Overall review of User Management and Fujitsu are on target with the Project Plan. Including in this is the backend SAP applications. Active Directory is included here with the exception of TACACS+ for networks which is a separate service improvement programme. F/C 31st October 2011 •The process for administering this process is out for review within Fujitsu and once signed off will be cascaded through the POL account. F/C 31st October 2011 •A set of BAU Review Reports are being defined by PO Ltd for Fujitsu to report against to monitor the findings. These will be our controls, reported periodically, against the user administration controls. F/C 31st October 2011 •The processes for the management of SAP Accounts in cash centres is in the process of being implemented by POL **(Complete 09/09/11)**	On target for completion by end October

FUJ00086948

Items 7 & 8

7. Low	Improvements to logical security settings for the infrastructure supporting Horizon on-line and POLSAP	•A review of Architectural documents is being undertaken and will continue as part of BAU and Fujitsu's Document Management Process. **(Complete)** •The implementation of a Pen Test Regime is required as part of BAU. Contractually this is not a requirement on Fujitsu but a CCN has now been agreed for a call off budget. Date to be determined when the PEN test will be undertaken. This is an internal Fujitsu resource to be assigned. The scoping of new projects has, where applicable, included PEN tests as a requirement.	[redacted]
8. Low	The RM Group Information Security Policy requires strengthening for password parameters, complexity, frequency of change etc.	•The Amendment of Post Office Account Security Policy is completed and out for review with both Fujitsu and POL On approval a cascade will be sent to all users advising them of changes to the policy and a set of guidelines provide. F/C 31st October 2011. •The robustness of the password strength across Active Directory will be included in the scope of the Pen Test (see point 7).	[redacted]

FUJ00086948

Items 9 & 10

9. Medium	Review of generic privileged accounts as there is evidence of multiple generic privileged accounts and passwords were being shared.	•This is part of the Overall review of User Management and Fujitsu are on target with the Project Plan. Including in this is the backend SAP applications. Active Directory is included here with the exception of TACACS+ for networks which is a separate service improvement programme. F/C 31st October 2011 •A set of BAU Review Reports are being defined by PO Ltd for Fujitsu to report against to monitor the findings. These will be our controls, reported periodically, against the user administration controls. F/C 31st October 2011 •All user management on the POL Account is now administered through The POL Account Security Operations Team in accordance with the User Management Procedure **(Complete)**	[redacted]
10. Low	Improvements to the problem and incident management process to ensure they are classified correctly.	•The problem and incident management document / process has been reviewed and updated. Need to discuss with Service Management in POL their needs from this process and the potential for a report from the framework solution. **(Complete for documentation)** •A Review of this area is regularly undertaken in most of the audits of the Account and any remedial actions found are rectified.	[redacted]