POL00142944

Management Response and summary of E&Y Financial Audit findings 2011/12

	New Findings 2011/12		Comment
1	**Strengthen user admin process** 4x HNG findings – 2x findings – resolved through initiation of revised process 4x SAP findings all in Cash Centre – responsibility of CC Managers	2012 Med	*Recommended management response* As part of the improvement process, and due to findings from last year's audit a standardised access control management process has been implemented by Fujitsu for both HNG and POLSAP (excluding Cash Centres). This process requires further evaluation to assess performance, but has already been proven to catch outstanding anomalies. Mitigating controls are in place through the use of iKeys and issuing procedures. Fujitsu HR are now part of the process in access revocation.
2	**Strengthen password parameters** No standard security policy exists across all accounts / applications	2012 Low	*Recommended management response* E&Y have acknowledged that password weaknesses in the application, operating system and database level are further protected to some extent by the network and Active Directory password controls POL to review multiple security policies and standardise where appropriate, to provide a suitable cross-reference of parameter setting across multiple systems, landscapes and suppliers

Ernst & Young have allocated findings against the categories utilised in last year's audit. While these have been assessed as closed by POL (and RMG Internal Audit) new, lesser findings are being reported against these categories.

	Prior year - open		Comment
1	**Strengthen the change management process** SAP – 14x anomalies where name evidence required HNG – 35x anomalies raised 26x discounted as null findings (due to being maintenance changes) 9x findings prior to implementation of new process	2011 high	*Recommended management response* E&Y review of change management processes did reflect improvements since the prior year audit Further clarity to be provided to the auditor regarding responsibility of authorisation of changes according to category (ie maintenance change, antivirus etc.) – 26x null findings. Service Improvement process implemented in Nov/Dec 2011 to resolve other findings. E&Y to provide amended RAG status
2	**Review of privileged access** SAP – 2x findings POL Information Security – to assess whether appropriate to shared service environment HNG – 2x findings POL Information Security – to assess whether appropriate to shared service environment	2011 high	*Recommended management response* E&Y review of privileged access to IT functions across the in-scope applications and their supporting infrastructure did reflect improvements, particularly around POLSAP privileged access As part of the improvement process, and due to findings from last year's audit a standardised access control management process has been implemented by Fujitsu for both HNG and POLSAP (excluding Cash Centres). This process requires further assessment to ensure performance, but has already been proven to catch outstanding anomalies Mitigating controls are in place through the use of iKeys and issuing procedures. Reporting and evidence has been standardised in BAU reports for Privileged Access utilisation. As part of the iSMF BAU process management reviews assess adequacy and regularity of the controls in place. POL Information Security to review appropriateness of access against best practise and centre of excellence models E&Y to provide amended RAG status
3	**Implement periodic user access review and monitoring controls** HNG – 2x findings – quarterly	2011 Med	*Recommended management response* **Objection** to the statement – ' no process in place to periodically validate user access appropriateness to the HNGX estate' A process does exist, including a quarterly review , with communication & management via Information Security Management Forum (iSMF).

POL00142944

	review not demonstrated SAP – 1x finding – evidence of review not retained		Implementation of the new process took place in October 2011, regular access management reviews have been performed, with the exception of the data centre physical access in Ireland (which was in the midst of a Service improvement plan) and was unable to be evidenced to the E&Y Audit team. Processes to be reviewed and communicated and evidence to be retained. E&Y to provide amended RAG status
4	**Strengthen the user administration process** SAP – 6x findings – regarding Cash Centre manager authorities HNG – 4x findings 2x findings prior to (and captured by) new process implemented October 2011	**2011 med**	*Recommended management response* E&Y examination of the user administration process for the applications in scope reflected some improvements since the previous year audit SAP – Cash Centre Manager's authorising responsibility to be assessed and confirmed by Information Security as appropriate, with recommendations on segregation of duties. The existing review process to be assessed to ensure appropriateness of controls regarding Cash Centre authorisation E&Y to provide amended RAG status
5	**Improvements to logical security settings** 2x Linux findings 2x Oracle findings Fujitsu / POL Information Security to confirm whether this is appropriate to shared service environment	**2011 Low**	*Recommended management response* E&Y review of the logical security settings for the infrastructure supporting the applications in scope reflected improvements, including the remediation of the logical security weaknesses noted for the Linux platforms in the prior year Process currently in place to continue. Fujitsu will perform a periodic scan of passwords to be made as part of a regular Pen Test Exercise invoked by PO Ltd Security. Findings and exceptions outside of best practice to be raised at the regular embedded BAU monitoring sessions within the existing BAU governance process within POL and to be supported by the Audit Control Governance Board E&Y to provide amended RAG status
6	**Strengthen password parameters** Conflicting security policies	**2011 Low**	*Recommended management response:* E&Y review of the password configurations for the in-scope applications and the infrastructure supporting these applications reflected some improvements since the prior year audit Auditors do not appear to recognise the complexity of the estate in line with their recommendation. Limitations exist due to the complexity of multiple systems and it is inappropriate to apply a single standard as suggested. POL to review multiple security policies and standardise where appropriate, otherwise provide a suitable cross-reference of setting across multiple systems, landscapes and suppliers. E&Y to provide amended RAG status
7	**Review of generic privileged accounts** Centre of Excellence authorities / responsibilities Fujitsu / POL Information Security have confirmed that this is appropriate to shared service environment (agreed to by RMG Internal Audit - review 2012)	**2011 med**	*Recommended management response* E&Y review of privileged access to the in-scope applications and their supporting infrastructure reflected some improvements in the use of shared privileged accounts Process currently in place to continue Monitoring and communication will be provided to POL through the regular embedded BAU process to ensure access control management is robust. POL Information Security to confirm best practise approach and appropriateness of access rights E&Y to provide amended RAG status