FUJ00086969

Observation from E&Y audit	Proposed Management Response
Management Summary	The management report shows considerable improvement to the report from the 2010/11 Ernst & Young annual audit report. Management has made significant improvement across a number of areas and have closed out a large number of actions and improved in those that remain an observation this year. There are no findings of a high rating but management recognise the observations and will work to improve our controls and processes in line with our response.
1. Privileged Access. • Conduct a review of privileged access for in scope applications (HNG and SAP) • Revisit the need to grant access at SAP_ALL and SAP_NEW levels • Consider creating system accounts to run scheduled jobs for POLSAP • Periodic review of the activities where SAP_ALL and SAP_NEW are retained. • Implement monitoring controls for 3rd party suppliers.	HNG Management have significantly improved the processes around 'Privileged Access' since the 2010/11 Ernst & Young audit. There are a number of controls in place to monitor system privileges. The levels of privileges required to maintain the infrastructure and service are deemed appropriate. A standardised approach to access control now exists including reporting for Privileged Access Utilisation. Further mitigating controls are in place through the use of iKeys and issuing procedures. The POL Information Security Management Forum reviews the adequacy and controls in place regularly as part of its BAU function and reviews appropriateness of access against best practice for centre of excellence models. Management considers these controls to be appropriate at this point and considers this recommendation closed with no further action to be taken. This will be signed off as an acceptable risk by the POL Risk & Compliance committee. **POLSAP** Management accept the risk where SAP_ALL and SAP_NEW accounts have been assigned. This accepted working practice facilitates timely maintenance of our 24/7 service. This will be signed off as an acceptable risk by the POL Risk & Compliance committee. Review and Management of privileged access through these accounts is undertaken with all requests being approved via POL Service Management and reviewed on a monthly basis with the suppliers and POL Information Security. The use of privileged accounts for scheduled jobs, the process for scrutiny of this use and of dialogue use will be reviewed to assure ourselves that the appropriate controls are in place.

FUJ00086969

	Action 1. POL to review the existing process for monitoring the accounts identified in this report. Owner Richard Barber. Target completion date 31/07/2012.
2. User Admin Process. • Strengthen the HNG user admin process to retain approval documentation for access to the HNG estate • Strengthen the POLSAP user admin process to retain approval documentation for temporary set up for cash centres. • Consider a monitoring process for temporary set up for cash centres. • Re-communicate to cash centre managers that the standard process should be followed for permanent access modifications for SAPADS. • Implement a monitoring process for privileged users within cash centres. • Where user admin is controlled by a 3rd party ensure adequate monitoring controls. • For HNG and POLSAP strengthen the process for revocation of access when employees contracts are terminated.	**HNG** The process managing the User Admin process has been improved since the last audit. However, we will monitor the process regarding retention of that the documentation supporting request, set-up and approval. **Action 2.** Fujitsu will review the process regarding documentation retention and conduct internal audit. Owner Bill Membery. Target completion date 31/08/2012. **Action 3a.** Fujitsu will review the Joiner/Leaver/Transfer process. Owner Mark Arnold. Target completion date 31/08/2012. **Action 3b.** Findings to be reviewed with POL/POA leadership and course of action/next steps agreed 30/11/2012 **POLSAP** The administration process within Cash Centres has been improved following the last audit. However we will review the process for retention of documentation supporting the request, approval and set-up of temporary assignments to cash centre users. Additionally we will re-communicate to cash centre managers that the standardised process for user administration should be strictly followed and we will consider a monitoring process as part of this review both within POL and with 3rd party suppliers. **Action 4.** Review the process for documentation retention of temporary assignments to cash centre users and consider and determine if a monitoring process of cash centre approvals and 3rd party suppliers is required. Owner Sid Hadadi. Target Completion date 30/05/2012 **Action 5.** Communication to cash centre managers of the requirement to follow the standardised process for user administration. Owner Sid Hadadi. Target Completion date 30/05/2012
3. Change Management Process.	Management have improved the process regarding change management since the last audit. However, both POL and Fujitsu

FUJ00086969

• To enhance the change management process by retained evidence of authorisation, testing and approval to promote accountability. • Define the responsibilities of all parties involved. • Increase involvement in the change management process specifically for fixes and maintenance changes. • Describe the overall change management process within documentation. • Implement controls to ensure that 3rd party service providers are in place and in operation.	will amend their processes to ensure recording the name of the individual authorising, testing or approving changes as identified by the audit this year. POL does not always engage in the authorisation, testing and approval of maintenance changes or fixes as these are often BAU maintenance of the system (e.g. anti virus updates etc.) However, POL will produce a policy that states what POL must approve in this regard to offer clarity on the matter. POL have a document change process described in the Manage Improvement & Change document. Our suppliers have there own processes, but all suppliers follow a change process for introducing change. Management considers this position to be acceptable. This will be signed off as an acceptable risk by the POL Risk & Compliance committee. **Action 6.** POL to amend processes so that names are recorded in the authorisation, testing and approval process of changes. . Owner Sid Hadadi. Target Completion date 30/05/2012 **Action 7a.** Fujitsu will review process. Owner Mark Arnold. Target Completion date 31/08/2012 **Action 7b**. Findings to be reviewed with POL/POA leadership and course of action/next steps agreed 30/11/2012
4. Periodic user access reviews and monitoring controls. • To consider the implementation of a periodic review of appropriate access for HNG and POLSAP.	Although POL recognises Ernst & Young's recommendation both POL and Fujitsu agree that the existing process we have in place is sufficient at this point for its purpose and consider this recommendation closed. This will be signed off as an acceptable risk by the POL Risk & Compliance committee.
5. Generic Privileged Accounts. • To consider a review of generic privileged accounts and supporting infrastructure to determine if they can be replaced by individual accounts.	The process and use of generic privileged accounts known to a number of users in the various teams will be reviewed by both POL Head of Information Security and Fujitsu's Chief Information Security Officer. If it is deemed acceptable that these practices are within our level of risk then we will state that and close this recommendation. This will be signed off as an acceptable risk by the POL Risk & Compliance committee. **Action 8.** POL Head of Information Security and Fujitsu Chief Information Security Officer to review the existing practice with

FUJ00086969

• To consider monitoring controls to help ensure robust security practices are in place, particularly 3rd party suppliers.	regard to generic password usage and deem if an acceptable risk or not. Owner. Richard Barber and Howard Pritchard. Target Completion Date 31/07/2012.
6. Password parameters. • Review and update the 'RMG Security Policy' to meet the generally accepted password settings as described in the management letter. • Consider one single policy rather than multiple policies and guidelines. • Configure network, application and infrastructure components in line with the policy.	With regards to POL having multiple security policies, the POL Information Security Management Forum will review all security policies within the POL domain annually as part of its BAU role. As a result of the 2010/11 audit performed POL accepts the risk of these multiple security policies. This will be signed off as an acceptable risk by the POL Risk & Compliance committee. POL does not own the RMG Information Security policy. Under the agreement between POL and RMG for Separation POL must abide by RMG policies for shared infrastructure and systems until Separation is completed, in March 2014 at which point POL will review and implement appropriate policies on an annual basis. Until that time, Management consider the confirmation of the network, application and supplier infrastructure to be appropriate for the policy requirements. **Action 9.** POL to review annually the multiple information security policies through the Information Management Security Forum. Owner Richard Barber. Target Completion date 31/5/14.
7. Logical Security Settings. • To consider specific encrypted password settings for all Oracle databases and disabling the default administrator account and creating a new one with a strong password. • To consider monitoring controls to help ensure robust security practices are in place, particularly 3rd party suppliers.	POL and Fujitsu do not consider this observation with regard to Logical Security Settings to be a risk. However, both POL Head of Information Security and Fujitsu's Chief Information Security Officer will review the controls at the Information Security Management Forum and confirm the currently accepted position. This will be signed off as an acceptable risk by the POL Risk & Compliance committee. **Action 10.** POL and Fujitsu to review the controls around Logical Security Settings and deem if this risk is acceptable. Owner Richard Barber. Target Completion Date 31/07/2012.