

EY Mgt Letter – IT update



- Overall progress from the 2010/11 report but still improvements required
- EY needed to rely on additional testing in security and change control to cover full year
- Significant change increases risk for coming years
- Key areas raised
 - Privileged user access
 - User admin process
 - Change management
 - Periodic user reviews & monitoring
 - Generic privileged accounts (repeat from last year)
 - Password parameters
 - Logical security settings (repeat from last year)



EY Mgt Letter - IT Audit update



- Status of findings
 - Management agreed in principal with EY
 - EY agreed with proposed management actions
- Next steps
 - CIO final approval of IT management actions
 - EY update and issue final management letter
 - Management/EY undertake a lessons learnt review
 - Monitoring and closing of the outstanding actions by POL and Fujitsu



EY Mgt Letter - IT Actions



- Privileged user access
 - Reduction of number of privileged users from last year
 - However still privileged access exists with limited controls in particular in POL SAP
 - Key actions:
 - Review to assess feasibility of devolving SAP_ALL by 30/08/2012
 - Following review aim to ensure privileged access is given on a strict business need, such as incidents and change requests raised and where given effective monitoring in place by 30/09/2012
- User admin process
 - Approval of users access not always evidenced
 - Removal of some users not always timely
 - Key actions:
 - Review of user admin process regarding approval and retention in conjunction with Fujitsu to assess feasibility and need for a monitoring process by 31/08/2012
 - Finding to be reviewed and next steps agreed by POL and POA (Fujitsu account management) by 31/10/2012



EY Mgt Letter - IT Actions



- Change management
 - Improvement from last year
 - Completeness of change request documentation such as approver names and requestors
 - Procedure for maintenance changes & evidence of testing and approval by POL
 - Key actions:
 - Amend procedure to ensure names of approver and tester recorded by 31/08/2012
 - Findings to be reviewed by POL and POA (Fujitsu account management) to confirm next steps/actions agreed .by 31/10/2012
- Periodic user reviews & monitoring
 - Improvement from last year
 - Reconciliation of user access approved to actual access on systems
 - Key actions:
 - Consider feasibility of a risk based periodic review process. and next steps by 31/07/2012



EY Mgt Letter - IT Actions



- Generic privileged accounts
 - Repeat from last year
 - Sharing of generic user accounts in SAP & HNG application and database environments
 - Key actions:
 - Review of generic user accounts with Fujitsu by 30/09/2012
 - Aim to reduce the use of generic privileged accounts and ensure appropriate but practical controls are in place by 30/09/2012
- Password parameters
 - Passwords not set in line with policy
 - Need to move from RMG to POL master IT security policies and maintain annually
 - Configure networks, applications and infrastructure components in line with policy
 - Key actions:
 - In line with separation programme review and implement appropriate information policies - ongoing and complete 31/5/2014
 - Annual review of security policies by 31/03/2013
 - Establish plan to ensure system owners are aware of relevant IT security policies and take responsibility for implementation including password configuration – ongoing & complete 31/5/2014



EY Mgt Letter - IT Actions



- Logical security settings
 - Repeat from last year
 - Password setting and encryption not enabled on SAP and HNG databases
 - Default admin accounts not disabled on active directory controlling HNG
 - Key actions:
 - Review password settings for the Oracle database and ensure effective password control implemented in line with policy, risk and practicality to the business by 30/09/2012

